أعمال المؤتمرات



الملتقى الوطني

آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري

الجزائر العاصمة 29 مارس 2017

ISSN 2409-3963



الفهرس

توطئة...

للوسائط التكنولوجية العديد من الإيجابيات كونها توفر الوقت ونفقات التواصل وتقرب المسافات إلا أن الاستخدام غير المشروع لها قد أدى إلى ظهور نوع جديد من الجرائم سميت بالجرائم الإلكترونية والتي تشكل مصدر خطر قد يهدد أمن الفرد والمجموعات والدول على حد سواء.

ورغم تطور المنظومة القانونية للجريمة الالكترونية في الجزائر إلا أن هذا النوع من الجرائم قد أثار إشكالات قانونية من حيث تعريفها وتحديد مصطلحاتها وأنواعها، في مقابل قلة الأحكام والاجتهادات القضائية في هذا الشأن.

وبهدف التوعية من مخاطر الوقوع ضحية للجريمة الإلكترونية، والتعريف بالوسائل المتاحة للتقاضي وآليات الشكوى لضحايا هذه الجرائم.

نظم مركز جيل البحث العلمي يوم٢٩ مارس٢٠١٧ بمقر الإتحاد العالمي للمؤسسات العلمية بالجزائر العاصمة ملتقى وطني حول " **آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري**"،وذلك بالتعاون العلمي مع مخبر بحث الحوكمة العمومية والاقتصاد الاجتماعي بجامعة تلمسان.

و قد شارك في الجلسات العلمية المغلقة أساتذة وباحثون من عدة جامعات جزائرية أثارت أوراقهم النقص والقصور الوارد في المنظومة القانونية الجزائرية فيما يخص تنظيم التعامل مع البيئة الإلكترونية، و مست إشكاليات هذا المؤتمر ومختلف محاوره المسطرة،على الشكل الآتي:

المحور الأول: الإطار المفاهيمي للجريمة الإلكترونية.

المحور الثاني: أنواع الجرائم الإلكترونية.

المحور الثالث: الحماية والوقاية من الجرائم الإلكترونية.

المحور الرابع: التشريعات الوطنية في مجال مكافحة الجرائم الإلكتروني.

المحور الخامس: الآليات الوطنية لمكافحة الجرائم الإلكترونية.

ولقد توصلت اللجنة العلمية للملتقى إلى صياغة جملة من التوصيات من أهمها نشر أعماله ضمن سلسلة أعمال المؤتمرات الصادرة عن مركز جيل البحث العلمي. ومن هذا المنطلق يضع المركز تحت تصرفكم أهم الأبحاث العلمية المشاركة بهذا الملتقى والتي التزمت بالمعايير الشكلية الموضوعة من قبل لجنته العلمية الموقرة، كمساهمة منه في إثراء المكتبات بالدراسات والبحوث العلمية التي تلتمس قضايا العصر ومتطلبات الواقع في العالم الإسلامي.

المشرفة العامة / د. سرور طالبي المل



ماهية الجريمة الالكترونية

أ. مختارية بوزيدي أستاذة بجامعة الدكتور مولاي الطاهر سعيدة- الجزائر

ملخص

الجريمة الالكترونية من الجرائم المستحدثة التي بدأت في الانتشار بشكل واسع في الآونة الأخيرة وقد اختلف الفقهاء في تعريفها؛ فهناك من عرفها على أنها كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية. كما وقع اختلاف في تسميتها إلى أن المصطلحات الأكثر شيوعا ودقة هي جرائم الكمبيوتر والجرائم الالكترونية. كما يتسم مجرم الجريمة الالكترونية بأنه متخصص وله القدرة الفائقة والمهارة التقنية.

أما فيما يتعلق بالحماية الجزائية للمعلوماتية فقد تبناها المشرع الجزائري بموجب القانون رقم٠٤-١٥ المعدل والمتمم لقانون العقوبات فقد جرم الدخول والبقاء الغير مشروع في نظام المعالجة الآلية للمعطيات وجريمة الاعتداءات العمدية على المعطيات الموجودة داخل النظام ألمعلوماتي وحدد لكل نوع من الجرائم السابق الذكر أركانها والعقوبة المقررة لها.

مقدمة

تطورت الظاهرة الإجرامية في العصر الحديث تطورًا ملحوظًا ومذهلا؛ سواء في شخصية مرتكبها أو أسلوب ارتكابها مع استخدام آخر ما توصلت إليه العلوم التقنية والتلتنولوجية. وقد تميز القرن العشرين باختراعات هائلة على المستوى التقني لعل من أهمها ظهور الحاسوب الالكتروني؛ ووجود ما يعرف بالإنترنت؛ وتعني شبكة الشبكات أي ربط شبكات الحاسوب الموجودة يبعضها البعض. وقد نشأت الانترنت نشأة عسكرية عام١٩٦٩ من أجل وزارة الدفاع الأمريكية " البنتاجون" ثم سرعان ما تحول استخدامه إلى المجال التعليمي سنة١٩٧٢ حيث أتيح استخدامه من قبل الجامعة الأمريكية.[1] وأخذت استخدامات الانترنت تتطور فيما بعد.

رغم الايجابيات التي وفرها النظام ألمعلوماتي في شتى الميادين إلا أنه لا يخلوا من بعض المخاطر، لأن المعلومة باعتبارها علم للمعالجة الآلية للمعطيات أصبحت تُثير عدة مشكلات من الناحية القانونية؛ إذا قد يساير استخدامها لارتكاب الجرائم عن بعد؛ وفي هذا الصدد تقول " روى جودسون" خبيرة بالمركز الوطني الأمريكي للمعلومات " لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديثة"[2]. أو قد تكون محلا للاعتداء وهو الأمر الذي استلزم تدخل المشرع الجزائري من أجل التصدي لمثل هذه الظواهر ومعاقبة مرتكبها انطلاقاً من مبدأ الشرعية وفقاً لأحكام المادة الأولى من قانون العقوبات

[1] كوثر سعيد عدنان خالد، حماية المستهلك الالكتروني، دار الجامعة الجديدة ، الإسكندرية، بدون طبعة، ٢٠١٢م، ص ٠١.

[2] آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه للنشر والتوزيع، الجزائر، الطبعة الثانية،٢٠٠٧م، ص ٦.

الجزائري التي تنص على " لا جريمة ولا عقوبة أو تدابير أمن بغير قانون"،[1] وتبعاً لذلك جرم بعض صور الجريمة المعلوماتية وعاقب مرتكبيها بموجب القانون رقم ٠٤-١٥ المؤرخ في ١٠ نوفمبر ٢٠٠٤ المعدل والمتمم لقانون العقوبات وتناولها تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من المواد ٣٩٤ مكرر إلى المادة ٣٩٤ مكرر٧ من قانون العقوبات؛ من أجل مسايرة التشريع للتطورات التكنولوجية وعدم استفحال وثيرة النمو المتسارع الذي تشهده الدول العربية منها الجزائر في استخدام النظم المعلوماتية فضلا عن العولمة والتبعية التكنولوجية.وكذا القانون رقم ٠٩-٠٤ المؤرخ في ٠٥-٠٨-٢٠٠٩ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.[2] من خلال هذه التعديلات نجد أن المشرع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية وأغفل الاعتداءات الماسة بمنتجات الإعلام الآلي والمتمثلة في التزوير ألمعلوماتي. ومن هذه المقدمة ارتأينا طرح الإشكالية التالية وهي ما مفهوم الجريمة الالكترونية؟ وما هي الحماية الجزائية للمعلوماتية التي أقرها المشرع الجزائري؟

مقدمة

المبحث الأول: مفهوم الجريمة الالكترونية

المطلب الأول: تعريف الجريمة الالكترونية

المطلب الثاني: أنواع الجريمة الالكترونية وأهدافها

المبحث الثاني: الحماية الجزائية للمعلوماتية من خلال النصوص المستحدثة

المطلب الأول: مفهوم نظام المعالجة الآلية للمعطيات

المطلب الثاني: جرائم الاعتداءات الماسة بالأنظمة المعلوماتية

خاتمة

---

[1] الأمر رقم ٦٦-١٥٦ المؤرخ في ١٨ صفر سنة ١٣٨٦ الموافق ل ٨ يونيو ١٩٦٦ المتضمن قانون العقوبات، الجريدة الرسمية، العدد ٤٩، المؤرخة في ٢١ صفر ١٣٨٦ الموافق ل ١١ يونيو ١٩٦٦م.

[2] القانون رقم ٠٩-٠٤ المؤرخ في ١٤ شعبان عام ١٤٣٠ الموافق ل ٥ غشت سنة ٢٠٠٩م المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد ٤٧، المؤرخة في ٢٥ شعبان ١٤٣٠هـ الموافق ل ١٦ غشت ٢٠٠٩م.

المبحث الأول

مفهوم الجريمة الالكترونية

إن جرائم الحاسبات الالكترونية أو كما تسمى بجرائم المعلوماتية لارتباطها بنظم المعالجة الآلية للمعطيات هي ظاهرة إجرامية حديثة النشأة؛ لتعلقها بتكنولوجيا الحاسبات الآلية فقد اكتنفها الغموض مما صعب عملية تحديد مفهومها وهذا ما سنحاول التطرق إليه من خلال هذه المبحث.

المطلب الأول

تعريف الجريمة الالكترونية

إن مسألة وضع تعريف للجريمة الالكترونية كانت محلاً لاجتهادات الفقهاء، لذا ذهب الفقهاء في تعريف الجريمة الالكترونية مذاهب شتى ووضعوا تعريفات مختلفة. ويتراوح تعريف الجريمة الالكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية.وتعرف الجرائم الالكترونية على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال.[1]

وهناك من عرفها على أنها الجرائم ذات الطابع المادي التي تتمثل فيكل سلوك غير قانوني من خلال استخدام الأجهزة الالكترونية ينتج منها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل السرقة أو إتلاف المعلومات الموجودة في الأجهزة، ومن تم ابتزاز الأشخاص باستخدام تلك المعلومات.[2]

لقد تعدت تعارف الجريمة الالكترونية فهناك من تناولها من الزاوية التقنية أو من الزاوية القانونية، وهناك من عرفها اعتمادا على وسلة ارتكاب الجريمة. كما عرفها الأستاذ جون فورستر بأنها" فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسة"[3]. كما أن هناك جانب من الفقه لا يهتم بالوسيلة أو موضوع الجريمة المعلوماتية ويعرفها بوصفها مرتبطة بالمعرفة الفنية أو التقنية باستخدام الحاسب الآلي؛ ولذلك عُرفت هذه الجريمة بأنها " أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"، وبذلك عرفها الدكتور هشام فريد رستم بأنها " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات اساسية لمرتكبه"[4].

تتكون الجريمة الالكترونية من مقطعيين هما الجريمة والالكترونية، ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات؛ أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الالكترونية فهي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت".[5]

ومن التعريفات التي وضعها أنصار الاتجاه الضيق أن الجريمة المعلوماتية هي " كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازماً من ناحية؛ وملاحقته من ناحية أخرى كما عرفها هذا الاتجاه بأنها" هي التي تقع على

---

[1] دياب موسى البداينة، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، ملتقى علمي بالمملكة الأردنية الهاشمية بتاريخ ٠٤-٠٩-٢٠١٤م، ص ٠٢.

[2] مجلة تكنولوجيا المعلومات، قسم نظم المعلومات، بدون دار النشر، وبدون سنة.

[3] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن، بدون طبعة، ٢٠١١م، ص ٢٩.

[4] عادل يوسف عبد النبي البشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، العدد السابع، الكوفة، ص ١١٣.

[5] دياب موسى البدانية، المرجع السابق، ص ٣.

جهاز الكمبيوتر أو داخل نظامه فقط". أما أصحاب الاتجاه الموسع يعرف الجريمة المعلوماتية بأنها " كل سلوك إجرامي يتم بمساعدة الكمبيوتر" أو هي كل جريمة تتم في محيط أجهزة الكمبيوتر".[1]

فقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا سنة٢٠٠٠ تعريف الجريمة الالكترونية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي،والجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".[2]

أما التعريف الدولي للجريمة الالكترونية فهو يعتمد في الغالب على الغرض من استخدام المصطلح؛ فهناك عدد محدود من الأفعال التي تمس السرية والنزاهة وبيانات الكمبيوتر وأنظمة تمثل جوهر الجريمة الالكترونية. كما أن هناك أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر بما في ذلك الأفعال المتصلة بجرائم محتويات الكمبيوتر.[3]

ثمة اختلاف كبير بشأن المصطلحات المستخدم للدلالة على الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر والانترنت، وهو اختلاف رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات.فابتداء من مصطلح استخدام الكمبيوتر، مرورا بمصطلح الاحتيال بواسطة الكمبيوتر، والجريمة المعلوماتية و جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر وجرائم التقنية العالية، إلى جرائم الهاكرز أو الاختراقات فجرائم الانترنت وأخيرا السيبر كرايم.[4]

من المصطلحات التي شاعت في العديد من الدراسات هو اصطلاح الجرائم الاقتصادية المرتبطة بالكمبيوتر وهو تعبير يتعلق بالجرائم التي تستهدف معلومات قطاعات الأعمال. أما عن اصطلاحي جرائم الكمبيوتر و الجرائم المرتبطة بالكمبيوتر و الجرائم الالكترونية فهذه المصطلحات تعتبر الأكثر دقة للدلالة على هذه الظاهرة بالرغم من أنهما ولدا قبل ولادة الشبكات وقبل الانترنت، تحديداً ليس لسبب إلا لكون الانترنت بالنسبة للمفهوم الشامل لنظام المعلومات مكون من مكونات هذا النظام، وأن النظام من جديد أصبح يعبر عنه باصطلاح نظام الكمبيوتر أو النظام ألمعلوماتي.[5]

المطلب الثاني

أنواع الجريمة الالكترونية وأهدافها

و لقد تنوعت الدراسات التي تحدد المجرم وشخصيته ومدى جسامة جرمه كأساس لتبرير وتقدير العقوبة في الجرائم المعلوماتية، على أنه لا يمكن أن يكون هناك نموذج محدد للمجرم ألمعلوماتي. وإنما هناك سمات مشتركة بين هؤلاء المجرمين يمكن إجمال تلك السمات في مجرم متخصص الذي له القدرة الفائقة في المهارة التقنية؛ ويستغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور أو الشفرات. أما المجرم عائد للإجرام فيتميز فيه المجرم ألمعلوماتي بأنه عائد

---

[1] محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، ٢٠١٤م، ص ١١٨.

[2] خالد عياد الحلبي، المرجع السابق، ص ٣٠.

[3] ذياب موسى البداينة، المرجع السابق، ص ٣.

[4] محمود إبراهيم غازي، المرجع السابق، ص ١٢٠.

[5] محمود إبراهيم غازي، المرجع السابق، ص ١٢٢.

للجريمة دائما فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات.[1]

أما المجرم المحترف له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهارته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال. أما المجرم الذكي فهو يمتلك هذا المجرم من المهارات ما يؤهله إن يقوم بتعديل وتطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب.[2]

تتنوع أعمار وأهداف منفذي الجريمة الالكترونية مع اختلاف دوافعهم فهناك من منفذي الهجمات الأطفال والمراهقين الذين تكون في الغالب دوافعهم لمجرد التسلية غير مدركين حجم الأضرار التي يقومون بها. وهناك المحترفون والمختصين والإرهابيين الذين من الممكن أن تحكم أعمالهم شركات ضخمة وتضر بدول كبيرة.[3]

وتتمثل أهداف الجريمة الالكترونية في التمكن من الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الإطلاع عليها أو حذفها أو تغييرها بما يحقق هدف المجرم، والتمكن من الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أو التلاعب بمعطياته. كما يتم الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم من خلالها بدافع مادي أو سياسي. وتحقق الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات اختراق وهدم المواقع على الشبكة العنكوبتية وتزوير وسرقة الحسابات المصرفية.[4]

أما عن أنواع الجريمة الالكترونية فهناك الجرائم ضد الأفراد وتسمى بجرائم الانترنت الشخصية مثل سرقة الهوية، أو سرقة الاشتراك في موقع شبكة الانترنت. أما النوع الثاني فيتمثل في الجرائم ضد الملكية وهو انتقال برمجيات ضارة المضمنة في بعض البرامج التطبيقية لتدمير الأجهزة أو البرامج المملوكة للشركات أو أجهزة الحكومية أو البنوك. أما النوع الثالث فهو الجرائم ضد الحكومات وتتمثل في مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الانترنت وهي ترتكز على تدمير الخدمات والبنية التحتية ومهاجمة شبكات الكمبيوتر وغالبا ما يكون هدفها سياسي بحت.[5]

لمبحث الثاني

الحماية الجزائية للمعلوماتية من خلال النصوص المستحدثة

استقر الفكر القانوني على ضرورة إيجاد نصوص خاصة لحماية المال ألمعلوماتي؛ وقد استجابت عدة دول لهذه الحاجة بسنها قوانين تناولت في طياتها تعريف الجريمة ألمعلوماتي وأنواعها وخصائصها وأركانها والعقوبات المقررة لها. وتُعتبر

[1] أمير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة وفاء القانو نية للنشر، الإسكندرية، الطبعة الأولى، بدون سنة، ص ١٢٠.

[2] أمير فرج يوسف، المرجع السابق، ص ١٢١.

[3] مجلة تكنولوجيا المعلومات، المرجع السابق، ص٢.

[4] مجلة تكنولوجيا المعلومات، المرجع السابق، ص ٣.

[5] مجلة تكنولوجيا المعلومات، المرجع السابق، ص ٤.

الولايات المتحدة الأمريكية أول الدول التي سنت قوانين خاصة بالجريمة المعلوماتية من أجل حماية المعلوماتية وتليها بعد ذلك الكثير من الدول منها كندا وألمانيا وأستراليا.

أما بالنسبة للمشرع الجزائري فقد تدارك مؤخرا الفراغ القانوني في مجال الجريمة المعلوماتية وذلك باستحداث نصوص تجريمية خاصة لقمع الاعتداءات الواردة على المعلوماتية بموجب تعديل قانون العقوبات الذي تمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم ٦٦-١٥٦ بإضافة القسم السابع المكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" من المادة ٣٩٤ مكرر إلى ٣٩٤ مكرر ٧ من قانون العقوبات؛ وكذا القانون رقم ٠٤٠٩ المؤرخ في ٢٠٠٤٩٨٠٥ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته. أما على المستوى الدولي فنجد أول اتفاقية حول الإجرام ألمعلوماتي كان بتاريخ ٢٠٠١١١٠٨ التي تضمن مختلف أشكال الإجرام ألمعلوماتي.[1] أما المشرع الفرنسي فقد تناولها في المواد ٣٢٣-١ إلى ٣٢٣-٧ من قانون العقوبات الفرنسي.

نجد أن المشرع الجزائري اتخذ هذه الإجراءات اللازمة من أجل مقاومة الجريمة المعلوماتية المنصوص عليها في الاتفاقية الأورومتوسطة المؤرخة في ٢٢ أفريل ٢٠٠٢، التي كانت تهدف إلى ربط الجهود بين الوحدة الأوربية والدول الأعضاء فيها ومابين الحكومة الجزائرية من جهة أخرى. وقد صادقت الجزائر مع الدولة الفرنسية في مجال الأمن ومكافحة الإجرام المنظم وذلك بتاريخ ٢٥ أكتوبر ٢٠٠٣ ودخلت حيز التنفيذ بموجب المرسوم الرئاسي رقم ٠٧-٣٧٥.[2]

المطلب الأول

مفهوم نظام المعالجة الآلية للمعطيات

وقبل أن نخوض في أنواع الجريمة المعلوماتية فلا بد علينا التعرض إلى مفهوم نظام المعالجة الآلية للمعطيات، فإن وجود نظام المعالجة البيانات أو المعالجة آلية للمعطيات بمثابة الشرط الأول الذي يلزم تحقيقه حتى يتم بحث ما إذا كان هناك اعتداء على نظم المعالجة الآلية للبيانات من عدمه. وقد عرفه مجلس الشيوخ الفرنسي " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي تربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية".[3] كما عرفتها المادة ١٤١ من القانون العربي النموذجي الموحد بأن نظام المعالجة الآلية للمعطيات هي " كل مجموعة مركبة من وحدة أو عدة وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة".[4]

أما جانب من الفقه يعرف نظام المعالجة الآلية للمعطيات بأنها علم قائم بذاته لأن كلمة معلوماتية هي مزج مختصر لكلمتين معلومة وكلمة آلية ومعناها المعالجة الآلية للمعلومة؛ ويفهم من المعطيات الفكرية آليا هي عمل البرامج والبيانات

---

[1] الاتفاقية الدولية حول الإجرام ألمعلوماتي أبرمت بتاريخ ٠٨-١١-٢٠٠١ من طرف المجلس الأوربي وتم وضعها للتوقيع مند تاريخ ٢٣-١١-٢٠٠١.

[2] المرسوم الرئاسي رقم ٠٧-٣٧٥ المؤرخ في ٢١ ذي القعدة عام ١٤٢٨ الموافق ل ١ ديسمبر ٢٠٠٧، الجريدة الرسمية المؤرخة في ٩ ديسمبر ٢٠٠٧، العدد ٧٧.

[3] قد أشار التعريف الفرنسي إلى العناصر المادية والمعنوية التي يتكون منها المركب أساس نظام المعالجة الآلية للبيانات وه ذه العناصر وردة على سبيل المثال لا الحصر.

[4] عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومه للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية، ٢٠١٣م، صر١٠٩.

الموجودة في الكمبيوتر وعلى شبكة الانترنت سواء كانت فنية أو أدبية أو علمية أو تجارية أو صناعية فهي تصنف كإنتاج ذهني لأصحابها.[1]

أما المشرع الجزائري تبنى التعريف الذي جاءت به اتفاقية الدولية للإجرام ألمعلوماتي،[2] بموجب أحكام المادة الثانية الفقرة ب من القانون رقم٠٩-٠٤ وأطلق عليها تسمية " منظومة معلوماتية" وعرفها بأنها" أي نظام منفصل أو مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبطة بقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا للبرنامج معين"

إن نظام المعالجة الآلية للمعطيات يقوم على عنصرين هما:

* يتكون من عناصر مادية ومعنوية التي يتكون منها المركب مثل الذاكرة، البرامج، المعطيات، أجهزة الربط...الخ وبما أن هذه العناصر واردة على سبيل المثال لا للحصر فإن ذلك يفتح المجال لإضافة عناصر جديدة أو حذف بعضها حسبما يستوجبه التطور التقني في هذا المجال.[3]

* أما العنصر الفني هو ضرورة خضوع النظام لحماية فنية فالرأي الغالب في الفقه الفرنسي؛ يري أن هذا الشرط ليس ضروريا، لأن وجوده لا يكون له سوى دور واحد وهو إثبات سوء النية من قام بانتهاك النظام والدخول إليه بطريقة غير مشروعة ويدخل في ذلك إثبات القصد الجنائي.[4] أما المشرع الجزائري فإن المبدأ المستقر فيه هو مبدأ الشرعية وعليه فإن عدم ذكر المشرع وعدم اشتراطه لشرط الحماية الفنية يعني أنه أراد استبعاد هذا الشرط صراحة. ومن الناحية العملية فإن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية ووجود مثل هذا النظام يساعد خاصة في إثبات أركان الجريمة وبصفة خاصة الركن المعنوي.[5]

يتضح أن هناك اختلاف واضح من حيث صياغة تعريف أنظمة المعالجة الآلية للمعطيات كون أن المشرع الجزائري جاء بتعريف عام وغير دقيق بالمقارنة مع المشرع الفرنسي، حيث يعتبر التعريف الذي جاء به المشرع الجزائري كان على صواب لأن أنواع الأنظمة المعلوماتية كثيرة ولا تنحصر فقط في أجهزة الكومبيوتر كما أشار إليها مجلس الأمة الفرنسي. كما أن النظام ألمعلوماتي في فرنسا محمي تقنيا، إلى أن المشرع الجزائري لم ينص صراحة على وجوب توافر حماية تقنية للنظام كي تقوم الجريمة.[6]

كما نجد أن المشرع الفرنسي لا يصوب مباشرة وبصفة منفردة على الكومبيوتر فقط فيما يخص المساس بنظام المعالجة الآلية للمعطيات، بل يشمل كل نظام أو جهاز بإمكانه المعالجة الآلية للمعطيات المعلوماتية؛ وعليه فإن شبكة الانترنت

[1] ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، الطبعة الثانية، ٢٠١٣م، ص ١٠٩.

[2] تعرضت إليه المادة الثانية من الاتفاقية الدولية للإجرام ألمعلوماتي؛ أمال قارة، المرجع السابق، ص ١٠١.

[3] سفيان سوير، جرائم معلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، سنة ٢٠١٠-٢٠١١، ص ٨٦.

[4] أما الرأي الآخر يرى ضرورة وجود نظام أمني لأن القانون يجرم الاعتداء على نظام الأمن المتضمنة في النظام ألمعلوماتي، ويستندون على عدة أسانيد منها أن الاعتداء على النظام الأمني شرط مفترض لقيام الجرائم التي تتعلق بنظم المعلوماتية، فضلا على أن التسليم برأي غالبية الفقه يعني التوسع في مجال التجريم فكل دخول غير مشروع يعد جريمة، عبد المجيد حباري، المرجع السابق، ص ١١٠.

[5] عبد المجيد جباري، المرجع السابق، ص ١١٠.

[6] نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في العلوم الجنائية، جامعة منتوري، قسنطينة، ٢٠١٢-٢٠١٣، ص٢٢.

تكيف على أنها نظام المعالجة الآلية للمعطيات، والبريد الالكتروني، ومصالح الخدمات التقنية للدخول إلى شبكة الانترنت أو تثبيت الصفحات أو مواقع الانترنت والبطاقة الالكترونية وبطاقة الاتمان البنكية فهم نظام معلوماتي.[1]

المطلب الثاني

جرائم الاعتداءات الماسة بالأنظمة المعلوماتية

بعدما تطرقنا إلى الركن المفترض في جرائم اختراق نظام المعالجة الآلية للمعطيات يأتي الحديث عن الركن المادي والمعنوي لكل جريمة.وأنواع الجرائم التي سنتطرق إليها هي:

١- جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

نص عليها المشرع الفرنسي في أحكام المادة ٣٢٣/١ من قانون العقوبات الفرنسي الجديد،[2] وكذلك المادة ٢ من الاتفاقية الدولية للإجرام ألمعلوماتي، أما القانون الجزائري فقد تناولها في أحكام المادة ٣٩٤ مكرر من قانون العقوبات.[3]

وباستقراء هذه النصوص نجد صورتين للركن المادي لهذه الجريمة وهي الصورة البسيطة والصورة المشددة؛ فالصورة البسيطة تقوم بمجرد الدخول أو البقاء الغير المشروع، فيقصد بفعل الدخول هو ظاهرة معنوية أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة آلية للمعطيات. ولم يحدد لنا المشرع الجزائري وسيلة الدخول،[4] فيستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر، وهذه الجريمة تقع من كل إنسان أيا كانت صفته وكفائتة المهنية والفنية فهي ليست من الجرائم ذوى الصفة.[5] والمشرع الجزائري يعاقب على الدخول المجرد إلى النظام ألمعلوماتي لأن مجرد الدخول إلى النظام حتى ولو لم يترتب على ذلك الدخول ضررًا أو فائدة طالما أن الدخول غير مشروع.[6]

وكقاعدة عامة إذا دخل الشخص في جزء أو كل لنظام معلوماتي فإنه يعاقب جزائيا بنفس العقوبة المقررة في نص المادة ٣٩٤ مكرر من قانون العقوبات الجزائري والمادة ٣٢٣-١ من قانون العقوبات الفرنسي.[7]

---

[1] وكذلك القرص النقال والقرص المرن والقرص المضغوط الذي يحتوي على قاعدة المعطيات والبرنامج ألمعلوماتي الذي يسمح الدخول إلى هذه القاعدة، زيادة على الأشرطة الممغنطة والأقراص المضغوطة أو أي دعامة مادية يتم فيها تخزين المعلومات والتي تحمل ضمنها برنامج خاص؛ نسيم دردور، المرجع السابق، ص ٢٣.

[2] Article 323-1 du code pénal française dalloz 107 edition paris 2010"le fait d'accéder ou de se maintenir frauduleusement dans tout ou parti d'un système de traitement automatise de données est puni d'un d'emprisonnement et de 15000 euros d'amende .
Lorsqu' il en est résulté soit la suppression ou la modification de données contenues dans le système soit une altération du fonctionnement de ce système la peine est de deux ans d'emprisonnement et de 30.000 euros d'amende"

[3] نص المادة ٣٩٤ مكرر من قانون العقوبات " يعاقب بالحبس من ٣ أشهر إلى سنة وبغرامة من ٥٠.٠٠٠ دج إلى ١٠٠.٠٠٠ دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة آذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة من ٦ أشهر إلى سنتين والغرامة من ٥٠.٠٠٠ دج إلى ١٥٠.٠٠٠ دج"

[4] يمكن للجاني الدخول باستعمال برنامج أو شفرة خاصة، كما يمكن له استخدام الرقم السري لشخص مسموح له بالدخول وكان المالك للنظام قد وضع قيودا على الدخول ولم يحترم الجاني هذه القيود أو كان الأمر يتطلب سداد مبلغ من النقود ولم يسددها الجاني، عبد المجيد جباري، المرجع السابق، ص ١١٠؛ آمال قارة، المرجع السابق، ص ١٠٧.

[5] سفيان سوير، المرجع السابق، ص ٨٨.

[6] ربيحة زيدان، المرجع السابق، ص ٤٩.

[7] نسيم دردور، المرجع السابق، ص ٢٨.

وبعدما تحدثنا عن الركن المادي لهذه الجريمة في صورتها البسيطة، نجد أن الركن المعنوي يكفي توافر القصد الجنائي العام وهو الدخول إلى النظام يجب أن يكون إرادي وليس خطأ أو بالصدفة؛ وبالتالي فإن هذا التصرف هو جريمة عمديه أي أن المجرم يكون على علم بأن الدخول إلى النظام غير مسموح به حتى يتسنى معرفة توافر سوء النية لدى المجرم، كما أن توافر نية الإضرار بالنظام غير ملزمة حتى تقوم الجريمة إذا لم يشترط المشرع قصد جنائي خاص.[1]

نجد أن القانون الفرنسي يعاقب على هذه الجريمة بالحبس بسنتين حبس و٣٠ ألف أورو أما القانون الجزائري فيعاقب عليه بالحبس من٣ أشهر إلى عام حبس والغرامة من ٥٠٠٠٠ دج إلى ١٠٠٠٠٠ دج.

أما فعل البقاء فهو التواجد داخل نظام المعالجة آلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، ويتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام؛ وقد يجتمعان ويكون البقاء معاقبا عليه وحده حين يكون الدخول إلى النظام مشروعا.[2] وقد اتجه غالبية الفقه إلى اعتبار هذه الجريمة هي جريمة سلوك مجرد، أي أنها تقع وتكتمل بمجرد الانتهاء من السلوك المكون لها والمتمثل في الدخول أو البقاء أي أن الركن المادي لتلك الجريمة لا يشترط أن يضاف إليه ضرورة التقاط معلومات أو أي شكل من أشكال الضرر إذا لم يشترط المشرع في نموذجها القانوني أي نتيجة إجرامية.[3]

تعتبر جريمة البقاء في النظام ألمعلوماتي من الجرائم المستمرة، فالجريمة تستمر كلما زادة مدة البقاء الغير مشروع داخل النظام وبالتالي استمرار الفعل الإجرامي واكتمال عملية البقاء الغير مشروع في النظام ألمعلوماتي. وتقام الجريمة بمجرد توافر القصد الجنائي العام؛ أي يكون الجاني على علم بأن ليس له الحق بأن يقوم بهذا التصرف أي البقاء ومع ذلك ارتكب الجريمة. وهذا ما قرره مجلس قضاء باريس في إحدى قراراته فاعتبر أن الجريمة لا تقوم إذا كان مشغل النظام لا يعلم وجوب الحصول على ترخيص للدخول والبقاء في النظام.[4]

يعاقب على فعل البقاء في صورته البسيطة بالحبس سنتين و٣٠ ألف أورو بالنسبة للقانون الفرنسي، أما المشرع الجزائر فالعقوبة تتراوح مابين٣ أشهر إلى عام حبس والغرامة من ٥٠٠٠٠ دج إلى ١٠٠٠٠٠ دج.

أما الصورة المشددة في هذه الجريمة فهي إما المحو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام إشغال المنظومة وفق نص المادة ٣٩٤ مكرر فقرة٢ من قانون العقوبات. ويكفي لتوافر هذا الظرف المشدد أن تكون هناك علاقة سببية مابين الدخول أو البقاء الغير المشروع وبين النتيجة التي تحققت وهي محو النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات وهذه النتيجة ذاتها هي التي اعتبرها المشرع الجزائري ظرفا مشددا وضاعف العقوبة وجعلها مشددة كما ورد فينص المادة ٣٩٤ مكرر الفقرة الثانية.[5]

نص المشرع الفرنسي على جريمة الدخول والبقاء الاحتيالي في الأنظمة المعلوماتية مع التأثير عليها في أحكام المادة ٣٢٣-١ فقرة٢ من قانون العقوبات الفرنسي. ويكون هذا التأثير السلبي على النظام إما بحذف أو تغيير لمعطيات المحتواة فيه أو إفساد سير النظام أو تخريبه. أما المشرع الجزائري فقد حصر تفسير التأثير بأنه تخريب نظام إشعال المنظومة أو النظام

---

١ نسيم دردور، المرجع السابق، ص ٣٢.

٢ ومن أمثلة ذلك إذا تحقق الدخول الى النظام بالصدفة أو عن طريق الخطأ أو السهو وكان على الشخص قطع وجوده وانسحابه فورا، أو في حالة تجاوزه المدة المسموح له البقاء فيها داخل النظام وكذلك في حالة استخدام الغير المشروع للبطاقات الممغنطة إما لسرقتها أو تزويرها ثم استخدامها؛ سفيان سوير، المرجع السابق، ص ٨٩.

٣ سفيان سوير، المرجع السابق، ص ٩٠.

٤ نسيم دردور، المرجع السابق، ص ٣٣.

٥ عبد المجيد جباري، المرجع السابق، ص ١١٣.



ألمعلوماتي. وبالتالي إذا نتج عن الدخول الغير مشروع حذف أو تغيير معطيات المنظومة دون التأثير عليها فالقاضي الجزائي الجزائري لا يعاقب عليه ويخضع ذلك لسلطة التقديرية للقاضي.[1]

تعتبر هذه الجرائم من الجرائم العمدية التي يتطلب لقيامها توافر القصد الجنائي العام لدى الجاني بعنصريه هما العلم والإرادة، فإذا أثبت الجاني انتفاء العلاقة السببية بين السلوك الإجرامي ألا وهو الدخول أو البقاء غير المشروع والنتيجة الإجرامية، كأن يثبت أن تعديل محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث مفاجئ انتفى السلوك الإجرامي والقصد الجنائي لدى الجاني[2].

يعاقب على فعل الدخول والبقاء في صورته المشددة بالحبس لمدة ٣ سنوات والغرامة ب٤٥ ألف أورو بالنسبة للمشرع الفرنسي، أما المشرع الجزائري يعاقب بالحبس من ٦ أشهر إلى سنتين حبس والغرامة من ٥٠.٠٠ دج إلى ١٥٠.٠٠ دج وفق أحكام المادة ٣٩٤ مكرر الفقرة الثانية من قانون العقوبات.

٢- جريمة إعاقة أو تحريف تشغيل نظم المعالجة الآلية للمعطيات

نصت على هذا الفعل قانون العقوبات الفرنسي في أحكام المادة ٣٢٣/١ من قانون العقوبات وكذا المادتين ٥ و٨ من الاتفاقية الدولية للإجرام ألمعلوماتي؛ أما المشرع الجزائري فلم يتطرق لهذا النوع من الجرائم.

يقصد بالتعييب هو الإفساد وهو لا يعطل نظام معالجة البيانات لكنه يجعل هذا النظام غير قادر على الاستعمال السليم؛ ويعطي نتائج غير تلك التي كان من الواجب الحصول عليها. ولم يشترط المشرع وسيلة معينة لتعطيل أو التوقيف فقد يتم بإدخال فيروس " مثل فيروس جصان طروادة" على البرنامج أو تعديل كلمة السر. كما يتحقق الإفساد عن طريق الإتلاف أو تخريب العناصر المادية في النظام. وهذه الجرائم من الجرائم العمدية التي تقوم على توافر القصد الجنائي العام بعنصريه هما العلم والإرادة.[3]

٣- جريمة الاعتداءات العمدية على المعطيات الموجودة داخل النظام ألمعلوماتي

نصت عليه المادة ٤٤٦٢ من قانون العقوبات الفرنسي القديم ولكن المشرع عاد ونص على مضمون ذات النص في المادة ٣٢٣/٣ من قانون العقوبات الجديد، وكذلك المواد ٣، ٤، ٥، ٨ من الاتفاقية الدولية للإجرام ألمعلوماتي. أما المشرع الجزائري فنص على ذلك في أحكام المادة ٣٩٤ مكرر ١ من قانون العقوبات، [4] وعليه فإن لهذه الجريمة صورتين تتمثل الأولى في الاعتداءات العمدية على المعطيات الموجودة داخل النظام أما الصورة الثانية تتمثل في المساس ألعمدي بالمعطيات خارج النظام.

أ- الاعتداءات العمدية على المعطيات الموجودة داخل النظام وتتجسد في إحدى الأفعال الثالثة وهي الإدخال، المحو، التعديل، مع ملاحظة أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداها فقط لكي يقوم الركن المادي. كما أن هذه الأفعال تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة أو محو أو تعديل معطيات موجودة من قبل.

---

[1] نسيم دردور، المرجع السابق، ص ٣٣.

[2] ربيحة زيدان، المرجع السابق، ص ٥١.

[3] عبد المجيد جباري، المرجع السابق، ص ١١٤.

[4] نص المادة ٣٩٤ مكرر ١ من قانون العقوبات الجزائري" يعاقب بالحبس من ٦ أشهر إلى ٣ سنوات وبغرامة من ٥٠٠.٠٠٠ دج إلى ٢.٠٠٠.٠٠٠ دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش التي يتضمنها"

نجد أن المشرع الجزائري خلاف لنظيره المشرع الفرنسي فقد أعطى تعريفا للمعطيات المعلوماتية من خلال المادة٢ ٠ فقرة ج من القانون رقم٩ ٠٤ ٠ والتي تنص على "....

معطيات معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".[1]

من خلال هذا التعريف نجد أن المعطيات المعلوماتية هي كل معلومة مهما كانت طبيعتها بشرط أن تكون في شكل معلوماتي أو إلكتروني والتي قد تلعب دور مهم في تشغيل منظومة معلوماتية. وكل من التشريع الفرنسي والجزائري اعتبر النظام ألمعلوماتي مال من خلال تجريم المساس به في قسم الجرائم ضد الأموال.[2]

يتحقق فعل الإدخال بإضافة معطيات جديدة على الدعامة الخاصة به سواء كانت خالية أم يوجد عليها معطيات من قبل.[3] ويكفي توافر القصد الجنائي العام لقيام الجريمة؛ فيجب أن يكون هذا التصرف الغير مشروع إرادي أي توافر النية الجرُمية بمعنى الإضرار بالمعطيات المعلوماتية الموجودة في النظام ألمعلوماتي المملوك للغير؛ ومع العلم بأن هذا التصرف غير مسموح به وهنا المشرع لم يشترط قصد جنائي خاص.[4]

يعاقب عليها المشرع الفرنسي ب٥ سنوات حبس والغرامة ب٧٥ ألف أورو وفق نص المادة٣٢٣-٣ من قانون العقوبات الفرنسي. أما المشرع الجزائري فيعاقب عليها بالحبس من٦ أشهر إلى٣ سنوات وبغرامة من٥٠٠.٠٠٠ دج إلى٢.٠٠٠.٠٠٠ دج وفق نص المادة٣٩٤ مكررا١ من قانون العقوبات الجزائري.

أما فعل المحو يقصد به إزالة جزء من المعطيات المسجلة على الدعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.[5]وفعل التعديل يقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، وقد يتم التلاعب في المعطيات عن طريق استبدالها أو عن طريق التلاعب في البرنامج وذلك بإمداده بمعطيات مغايرة تؤدي إلى نتائج مغايرة عن تلك التي صمم البرنامج لأجلها.[6]

كقاعدة عامة فإن المحو أو التعديل للمعطيات الموجودة في النظام كصورتين للركن المادي في جريمة الاعتداء على نظام المعالجة الآلية للمعطيات، يتم عن طريق برامج خبيثة تتلاعب في هذه المعطيات وذلك بمحوها كليا أو جزئيا أو بتعديلها باستخدام القنبلة المعلوماتية الخاصة بالمعطيات. وان فعل الإدخال أو المحو أو التعديل وارد على سبيل الحصر لا على سبيل المثال.[7]

أما عن فعل الإدخال بطريق الغش معطيات معلوماتية في النظام ألمعلوماتي؛ فيتحقق هذا الفعل بمجرد إدخال معطيات معلوماتية مهما كان نوعها؛ مثل فيروس معلوماتي أو مستندات أو بيانات أو برامج في النظام ألمعلوماتي محل الجريمة،

---

[1] القانون رقم ٠٩-٠٤.

[2] نسيم دردور، المرجع السابق، ص ٣٩.

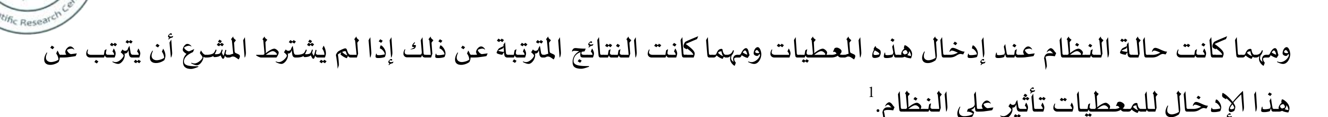
[3] ومن صور إدخال المعلومات المصطنعة " اختلاس النقود عن طريق الغش ألمعلوماتي" ويتحقق كذلك فعل الإدخال في القرص الذي يتمكن فيه الحامل الشرعي لبطاقة السحب الممغنطة و التي تسحب النقود من البنوك وتحديدا أجهزة السحب الآلي وذلك حين يستخدم رقمه الخاص السري للدخول كي يسحب مبلغا أكثر من ذلك المسموح به لصاحبه أو في حالة إدخاله لفيروس طروادة"؛ عبد المجيد جباري، المرجع السابق، ص ١١٦.

[4] نسيم دردور، المرجع السابق، ص ٤٠.

[5] سفيان سوير، المرجع السابق، ص ٩٤.

[6] عبد المجيد جباري، المرجع السابق، ص ١١٧.

[7] سفيان سوير، المرجع السابق، ص ٩٥.



ومهما كانت حالة النظام عند إدخال هذه المعطيات ومهما كانت النتائج المترتبة عن ذلك إذا لم يشترط المشرع أن يترتب عن هذا الإدخال للمعطيات تأثير على النظام.[1]

هذه الجرائم من الجرائم العمدية التي تقوم على القصد الجنائي بركنيه العلم والإرادة فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، وعلمه بأن نشاطه غير مشروع وأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات زيادة على توافر نية الغش، لكن هذا لا يعني توافر القصد لإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع علمه بذلك واتجاه الإرادة إليه.[2]ويعاقب مرتكبها بالحبس من ٦ أشهر إلى ٣ سنوات والغرامة من ٥٠٠٠٠٠ دج إلى ٢٠٠٠٠٠٠ دج وفق نص المادة ٣٩٤ مكررا ١ من قانون العقوبات.

ب- المساس العمدي بالمعطيات خارج النظام

نص عليه المشرع الجزائري في أحكام المادة ٣٩٤ مكرر ٢ من قانون العقوبات،[3]وكرس بموجبها المشرع الحماية الجزائية للمعطيات في حد ذاتها لأنه لم يشترط أن تكون المعلومة داخل نظام المعالجة آلية للمعطيات أو أن يكون قد تم معالجتها أليا.

نصت المادة ٣٩٤ مكرر ٢ الفقرة الأولى أن محل الجريمة يتمثل في المعطيات سواء كانت مخزنة في أشرطة أو أقراص أو معالجة آليا أو مرسلة عن طريق منظومة معلوماتية مادامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

في حين أن الفقرة الثانية من المادة ٣٩٤ مكرر ٢ من قانون العقوبات جرمت أفعال الحيازة الإفشاء، النشر، والاستعمال أيا كان الغرض من هذه الجرائم الواردة في القسم السابع مكرر من قانون العقوبات فقد يكون الهدف من ذلك المنافسة الغير المشروعة، الجوسسة، الإرهاب أو التحريض على الفسق.[4]

أما عن استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وذلك بالتصميم الذي نص عليه المشرع في أحكام المادة ٣٩٤ مكرر٢ الفقرة الأولى من قانون العقوبات إلى أن المشرع الفرنسي لم يتطرق إلى ذلك. وتتمثل جريمة التصميم لمعطيات معلوماتية مقرصنة في برمجتها بواسطة المعلوماتية؛ أي الكمبيوتر ومثال عن ذلك الفيروسات المعلوماتية وبرامج القرصنة التي يمكن أن تستعمل في ارتكاب الجرائم المعلوماتية إما ضد الأنظمة المعلوماتية أو المعطيات المعلوماتية في حد ذاتها. ويقصد بالمعطيات المعلوماتية المقرصنة هي المعطيات في شتى أنواعها " معطيات، أو بيانات، مستندات، برامج" ودورها الأساسي هو الإضرار بالأنظمة أو المعطيات المعلوماتية إذا فهي تتمتع بخاصية الإضرار بالأنظمة المعلوماتية.[5]

---

[1] نسيم دردور، المرجع السابق، ص ٤٢.

[2] عطاء الله، فشار ملتقى مغاربي حول القانون والمعلوماتية بعنوان مواجهة الجريمة المعلوماتية في التشريع الجزائري، ليبيا، ٢٠٠٩م، ص ٣٣.

[3] المادة ٣٩٤ مكرر ٢ من قانون العقوبات الجزائري " يعاقب بالحبس من شهرين الى ٣ سنوات وبغرامة من ١٠٠٠٠٠٠٠ دج إلى ٥٠٠٠٠٠٠٠ دج كل من يقوم عمدا وعن طريق الغش بما يلي:

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"

[4] سفيان سوير، المرجع السابق، ص ٩٥.

[5] نسيم دردور، المرجع السابق، ص ٤٢.

أما عن الركن المعنوي فهو قيام المجرم بعملية تصميم هذه المعطيات المقرصنة ولا يشترط طريقة معينة لتصميمها، كما لا يشترط استعمال هذه المعطيات في جرائم أخرى. يعاقب عليها بالحبس من شهرين إلى ٣ سنوات وبغرامة من مليون دج إلى ٥ ملايين دج وفق نص المادة ٣٩٤ مكرر٢ من قانون العقوبات الجزائري.

والبحث أو التجميع فهو قيام المجرم بعملية بحث أو استوردا عبر شبكات الاتصال المعلوماتية أو أي مصدر آخر. أو تجميع معطيات معلوماتية مقرصنة من الممكن استعمالها للمساس بالأنظمة أو المعطيات المعلوماتية السليمة. فإذا كانت هذه المعطيات لا تشكل ضرر على الأنظمة أو المعطيات المعلوماتية فلا تقوم الجريمة[1]؛ هذه القاعدة تطبق على الجرائم المنصوص عليها في المواد ٣٩٤ مكرر ٢ فقرة ١ من قانون العقوبات الجزائري، والمادة ٣٢٣-٣-١ من قانون العقوبات الفرنسي. وهي من الجرائم العمدية التي يتطلب لقيامها توافر القصد الجنائي العام.

يعاقب عليها بالحبس من شهرين إلى ٣ سنوات وبغرامة من مليون دج إلى ٥ ملايين دج وفق نص المادة ٣٩٤ مكرر٢ فقرة أولى من قانون العقوبات الجزائري.أما القانون الفرنسي لم يحدد بدقة العقوبة المقررة في هذه الحالة ويرجع ذلك لسلطة التقديرية للقاضي الجزائي وفق نص المادة ٣٢٣-٣-١ من قانون العقوبات الفرنسي، مع إمكانية تشديد العقوبة.

أما التوفير أو النشر فهو قيام المجرم بعملية توفير أو نشر معطيات معلوماتية مقرصنة؛ من الممكن استعمالها للمساس بالأنظمة أو المعطيات المعلوماتية السليمة، فإذا كانت هذه المعطيات لا تشكل خطر على سلامة الأنظمة أو المعطيات المعلوماتية فلا تقوم الجريمة. وتتم عملية النشر أو التوفير عبر شبكة الانترنت في أغلب الأحيان من خلال عرض على الجمهور الانترنت هذه المعطيات المجرمة؛ سواء من خلال تثبيتها في مواقع أو صفحات الانترنت قابلة للاستنساخ أو نشرها أيضا عن طريق البريد الالكتروني.[2]

يتطلب ركنها المعنوي توافر القصد الجنائي العام وأن يقوم الجاني بتوفير ونشر معطيات معلوماتية مقرصنة بطريقة عمدية ورغم علمه بأن هذه التصرفات غير مشروعة، كما لا يشترط توافر القصد الجنائي الخاص. وتقرر لها نفس العقوبة المقررة للجرائم السابقة وفق نص المادة ٣٩٤ مكرر٢ من قانون العقوبات الجزائري.

أما عن الجرائم المتعلقة بالمعطيات المعلوماتية المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية والمتمثلة في الحيازة والإفشاء والنشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم التي نص عليها المشرع الجزائري في نص المادة ٣٩٤ مكرر٢ الفقرة الثانية؛ أما المشرع الفرنسي فلم يتطرق إليها.

يتمثل الركن المادي لهذه الجرائم في قيام المجرم بعملية الحيازة، إفشاء، نشر أو إفشاء أو استعمال المعطيات المعلوماتية المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، وهذه المعطيات المتحصل عليها بطريقة غير مشروعة لم يشترط المشرع الجزائري أن تكون الوسيلة من الممكن استعمالها من جديد للمساس بأنظمة أو معطيات المعلوماتية السليمة[3]؛ فإذا كانت هذه المعطيات لا تشكل ضرر على الأنظمة أو المعطيات المعلوماتية ففي هذه الحالة لا تقوم الجريمة وهذه هي القاعدة المطبقة على كل الجرائم المنصوص عليها في المادة ٣٩٤ مكرر٢ من قانون العقوبات الجزائري والمادة ٣٢٣-٣-١ من قانون العقوبات الفرنسي.

---

١ نسيم دردور، المرجع السابق، ص ٤٣.

٢ نسيم دردور، المرجع السابق، ص ٤٤.

٣ نسيم دردور، المرجع السابق، ص ٤٥.

ويتطلب لقيام الركن المعنوي توافر القصد الجنائي العام وهو النية في الحيازة أو النشر أو استعمال المعطيات المعلوماتية المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم الخاص بالمساس بأنظمة المعالجة الآية للمعطيات؛ دون اشتراط توافر القصد الجنائي الخاص. وتطبق على مرتكبها نفس العقوبة المقررة في المادة ٣٩٤ مكرر ٢ الفقرة الأولى من قانون العقوبات الجزائري.

وهذه الجرائم يعاقب فيها كذلك الشخص المعنوي وفق نص المادة ٣٩٤ مكرر ٤ من قانون العقوبات. وتطبق العقوبات التكميلية إلى جانب العقوبات الأصلية والمنصوص عليها في نص المادة ٣٩٤ مكرر ٦ من قانون العقوبات؛ وعقوبة الشروع هي نفسها عقوبة الجريمة التامة وهو ما نص عليه المشرع في المادة ٣٩٤ مكرر ٧ من قانون العقوبات.

خاتمة

نختم هذه المداخلة بأن الجريمة المعلوماتية تكتسي أهمية بالغة فهي تساهم في التعرف على ظاهرة إجرامية جديدة؛ بدأت في الانتشار في معظم التشريعات المقارنة، ونظرًا لارتباطها بتكنولوجيا متطورة أدى إلى تميزها عن الجرائم التقليدية بدءا بتسميتها وصولا إلى الأفعال التي تدخل ضمن دائرتها.

وجدت صعوبة في وضع تعريف للجريمة المعلوماتية؛ فلقد تعددت التعريفات بخصوصها، فهناك من ارتكز على موضوع الجريمة في تعريفها، في حين هناك من ارتكز الوسيلة التي ترتكب بها الجريمة وهناك من اعتبرها أنها مكونة من مقطعين هما الجريمة والالكترونية. وكذلك اختلاف كبير بشأن المصطلحات المستخدمة للدلالة على هذه الظاهرة الإجرامية المرتكبة عن طريق الانترنت وأن اصطلاح جرائم الكمبيوتر والجرائم الالكترونية هي المصطلحات الأكثر دقة للدلالة على هذه الظاهرة.

اضافت إلى السمات التي يتميز بها المجرم الذي يرتكب الجريمة الالكترونية حيث يعتبر من الأشخاص الذين يتمتعون بنسبة عالية من المهارات والمعرفة والذكاء ويرتكب الجريمة في هدوء دون أن يلفت الانتباه على عكس المجرم التقليدي الذي يرتكب الجرائم التقليدية عن طريق العنف في أغلب الأحيان.

كما نجد أن تعديل قانون العقوبات بموجب القانون رقم ٠٤١٥ الذي كانت له الأهمية في تدارك النقص الذي كان موجود في التشريع العقابي الجزائري وذلك باستحداث القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات، فهو يعد قفزة في المجال التشريعي مواكباً للتشريعات المقارنة من خلال تجريمه للأفعال التي يرتكبها الشخص الطبيعي؛ وتحميل الشخص المعنوي المسؤولية الجزائية وتوسيع نطاق العقوبة بتجريم الشروع في هذه الجرائم بتجريمه حتى الأعمال التحضيرية في إطار الاتفاق الجنائي.

ينسم تعريف المشرع الجزائري للجرائم المعلوماتية بالقصور لعدم تحديد صور السلوك الإجرامي لأنه تبنى المفهوم الموسع للجرائم المعلوماتية من خلال أحكام المادة ٢ من القانون رقم ٠٤٠٩ التي نصت على أن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هيجرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات.

جرم المشرع الجزائري أفعال الدخول والبقاء الغير الشرعي داخل النظام ألمعلوماتي وتشديد العقوبة إذ ا ترتب عن ذلك المساس بالمعطيات أو بنظام التشغيل للمنظومة المعلوماتية والمساس أو تغريرها واستخدام المعطيات كوسيلة الارتكاب الجرائم المعلوماتية وحيازة وإفشاء ونشر واستعمال المعطيات المحصلة من هذه الجرائم.

رغم جهود المشرع الجزائري لسد الفراغ التشريعي لمواجهة هذه الجرائم إلا أن نصوصه لا تزال ناقصة لذلك نقترح بعض التوصيات وهي:

تفعيل أسلوب التوعية والتهذيب لدى مستخدمي شبكة الاتصالات العالمية" الانترنت" وحثهم على الاستخدام الأمثل لهذه التقنيات والتي من المفترض وجدت لخدمة الإنسان وليس لمضرته. وإصدار تشريعات جزائية جديدة قائمة لمواجهة الجرائم المعلوماتية وتحديد العقوبات المناسبة لها بغية حماية النظام ألمعلوماتي.

اعتماد الدقة والحبكة القانونية عند تحديد أنماط السلوك الإجرامي والابتعاد عن التعبيرات الغامضة، وعدم الاقتصار عند التجريم والعقاب على أنماط السلوك المحظور المرتكب حاليا بل يجب مراعاة الأبعاد المستقبلية لأن تكنولوجيا المعلومات والحواسيب في تطور سريع بل يكاد يكون مذهل.

لا يكفي مواكبة المشرع العقابي الجزائري لنصوص التشريعات المقارنة بدون تجسيدها من الناحية التطبيقية والاستعانة بمختصين وخبراء قادرين على تشخيص الجريمة والعمل على تكوين فرق من الضبطية القضائية لكي تختص بهذا النوع من الجرائم وتكوين قضاة مختصين في هذا النوع من الجرائم مع توفير كافة الوسائل المادية والتقنية اللازمة لأداء عملها.

يتعين على المشرع العمل على إبرام اتفاقيات دولية وثنائية على حد السواء من أجل تحديد الاختصاص القضائي والمتابعة والمحاكمة نظرا للطبيعة الجريمة الالكترونية باعتبارها متعدية الحدود وتطور أساليب ارتكابها مما يستلزم مراجعة وتطوير القوانين القائمة وإصدار المزيد من القوانين لتقوية الترسانة القانونية في هذا المجال.

تجنب الكشف عن أي معلومات تتعلق بهم مثل بطاقات الهوية، أو الهوية على موقع الانترنت.وعدم إرسال الصور عبر الانترنت أثناء التحدث مع الغرباء.و عدم الاحتفاظ بالبيانات الحساسة في الحاسب الآلي مثل البيانات المالية والشخصية.

حفظ نسخة احتياطية من الملفات والمجلدات بحيث أنه لو فقدت البيانات لابتلائها بالفيروسات يكون هناك نسخة منها. وعدم استخدام بطاقة الائتمان الخاصة في حالة عدم التأكد من أن الموقع آمن، فهدا الإجراء قد يحمي من التحايل والاستراق.

قائمة المصادر والمراجع

أولا: قائمة المصادر والمراجع باللغة العربية

١- المواثيق الدولية

- الاتفاقية الدولية حول الإجرام ألمعلوماتي أبرمت بتاريخ ٠٨-١١-٢٠٠١ من طرف المجلس الأوربي وتم وضعها للتوقيع مند تاريخ ٢٣-١١-٢٠٠١.

٢- القوانين

- القانون رقم ٠٩-٠٤ المؤرخ في ١٤ شعبان عام ١٤٣٠ الموافق ل ٥ غشت سنة ٢٠٠٩م المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد ٤٧، المؤرخة في ٢٥ شعبان ١٤٣٠هـ الموافق ل ١٦ غشت ٢٠٠٩م.

٣- الأوامر

- الأمر رقم ٦٦-١٥٦ المؤرخ في ١٨ صفر سنة ١٣٨٦ الموافق ل ٨ يونيو ١٩٦٦ المتضمن قانون العقوبات، الجريدة الرسمية، العدد ٤٩، المؤرخة في ٢١ صفر ١٣٨٦ الموافق ل ١١ يونيو ١٩٦٦م.

٤- المراسيم

- المرسوم الرئاسي رقم ٠٧-٣٧٥ المؤرخ في ٢١ ذي القعدة عام ١٤٢٨ الموافق ل ١ ديسمبر ٢٠٠٧، الجريدة الرسمية المؤرخة في ٩ ديسمبر ٢٠٠٧، العدد ٧٧.

٥- المراجع

- إبراهيم غازي محمود، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الإسكندرية،الطبعة الأولى، م٢٠١٤.

- جباري عبد المجيد، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية، ٢٠١٣.

- زيدان ربيحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، بدون طبعة، بدون سنة.

- سعيد عدنان خالد كوثر، حماية المستهلك الالكتروني، دار الجامعة الجديدة، لإسكندرية، بدون طبعة،٢٠١٢م.

بدون سنة. [١] - عياد الحلبي خالد، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن،بدون طبعة،٢٠١١م.

- فرج يوسف أمير، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، الناشر مكتبة الوفاء القانونية، الاسكندرية، الطبعة الأولى، بدون سنة .

- قارة آمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه للنشر والتوزيع، الجزائر،الطبعة الثانية، ٢٠٠٧.

ملتقيات علمية ومجلات

- فشار عطاء الله، ملتقى مغاربي جول القانون والمعلوماتية بعنوان مواجهة الجريمة المعلوماتية في التسريع الجزائري، بلبيا، سنة ٢٠٠٩ .

- موسى البداينة دياب، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، ملتقى علمي بالمملكة الأردنية الهاشمية، بتاريخ ٠٤-٠٩-٢٠١٤، الأردن.

- يوسف عبد النبي البشكري عادل، الجريمة المعلوماتية وأزمة الشرعية الجزائية، العدد السابع، الكوفة.

مذكرات

- دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في العلوم الجنائية، جامعة منتوري، قسنطينة، ٢٠١٢-٢٠١٣م.

-سوير سفيان، جرائم معلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، ٢٠١٠-٢٠١١م.

ثانيا: قائمة المصادر والمراجع باللغة الأجنبية

القوانين بالغة الأجنبية

Code pénal français Dalloz 107 Edition paris 2010.



جرائم الدفع الالكتروني وسبل مكافحتها

د. فاطمة الزهرة خبازي، جامعة الجيلالي بونعامة ، خميس مليانة .

الملخص:

في فترة قصيرة من عمر الزمن أستطاع الانترنت أن يكون الأداة الأهم في حياة معظم الأشخاص. حيث أصبح جزءا لا يتجزأ من تعاملاتنا اليومية وقد أتاح ظهور هذه الأداة الفرصة لمافيا الجرائم الإلكترونية للتجول خلالها دون رقيب أو حسيب . كما تمكن السرية والخصوصية التيتنطوي عليها لغة الكمبيوتر؛ اللصوص من نقل المعلومات الخطرة والمحظورة سواء معلومات مخابراتية أو خطط تخريبية أو صور سرية بمجرد الضغط على زر لوحة المفاتيح بدون أدنى مجهود وبدون الخوف من العقاب.

ومازال جميع أساتذة القانون على مستوى العالم عاجزين عن إصدار تشريع يحظر الجرائم الإلكترونية. خاصة وأن أدلة إثبات الجريمة يصعب التوصل إليها. ومن خلال هذه الورقة سنحاول مناقشة أشكال الجريمة الإلكترونية ومخاطرها وطرق الوقاية منها.

Summary:

In a short period of time, the age of the Internet manage to be the most important tool in the lives of most people. Where he became an integral part of our daily dealings of this tool it has allowed the emergence of the opportunity to mafia cyber crimes to wander through without supervision or control. Confidentiality and privacy inherent in the computer language also enables; thieves from the transport of dangerous and prohibited information either intelligence or subversive or confidential information Pictures plans by simply pressing a keyboard button without the slightest effort and without fear of punishment.

And still all the law professors in the world are unable to pass legislation that prohibits cyber crimes. Especially since evidence is difficult to prove the crime reached. Through this paper we will try to discuss forms of electronic and risks and methods of prevention of crime, through the following themes:

The first axis and means of electronic payment.

The second axis: the theoretical framework for electronic crime.

Axis III: ways to combat cyber-crime.

مشكلة البحث:

لقد أتاح ظهور الانترنت العديد من التسهيلات لحياة أفضل و أيسر. إلا أنها حملت معها في نفس الوقت مخاطر وجرائم مست العديد من الجوانب الحياتية، وسببت تقلبات خطرة من الناحية الاقتصادية.

بحيث يحاول المخترقون والعابثون الاستفادة قدر الإمكان من توسع استخدام الانترنت وذلك بنشر فيروساتهم المدمرة لتعطيل أجهزة الكمبيوتر الخاصة بالأفراد ومختلف القطاعات الخاصة والحكومية و تجميد الشبكة بكاملها. وقد يقومون باختراق الأنظمة و مسح البيانات والقيام بالسرقات الإلكترونية وانتحال الشخصية والابتزاز و نشر إشاعات عبر الانترنت.

وعليه سنحاول من خلال هذه الورقة التماس الإجابة على التساؤل الرئيسي والمتمثل في:

ما المقصود بجرائم الدفع الالكتروني وماهية الطرق المنتهجة للقضاء علها ؟

فرضيات البحث:

للإجابة على الإشكالية الرئيسة للبحث نفترض منذ البدايةِ ما يلي:

• الجرائم الالكترونية هي تلك الجرائم التي ترتكب عن طريق استخدام شبكة الانترنت.

• تتعرض الشركات في مختلف دول العالم إلى خسائر اقتصادية ضخمة نتيجة تعرضها للجريمة الالكترونية •

أول خطوة للقضاء على هذا النوع من الجرائم هو الوقاية منها من خلال التعريف بها وتوعية المجتمع بمخاطرها.

أهداف البحث:

تسعى هذه الدراسة إلى توضيح مفهوم جرائم الدفع الالكتروني و سبل مكافحتها كما تهدف إلى :

• توضيح مفهوم الجريمة الإلكترونية، ومميزاتها التي جعلتها تنمو بنحو متزايد.

•ذكر بعض الإحصائيات الخاصة بجرائم الدفع الالكتروني.

•طرق مكافحة الجرائم الإلكترونية وخاصة تلك المرتبطة بالأموال.

أهمية البحث:

تنبع أهمية هذه الدراسة من الأهمية البالغة لموضوع الجريمة الالكترونية ومدى تأثيرها على وسائل الدفع الالكترونية . بالإضافة إلى ما يمكن أن تقدمه هذه الدراسة للباحثين في هذا المجال، في التعرف على هذا النوع من الجرائم، وكيفية معالجتها.

منهجية البحث:

بالنظر لطبيعة الموضوع محل الدراسة فانه سيتم انتهاج المنهج الوصفي لتوصيف مصطلح الجريمة الالكترونية، ووسائل الدفع الالكترونية. كما سيتم الاعتماد على المنهج التحليلي لتحليل الأرقام المعلقة بالموضوع محل الدراسة.

محاور البحث:

المحور الأول: الدراسات السابقة.



المحور الثاني: وسائل الدفع الالكتروني.

المحور الثالث: الإطار النظري للجريمة الالكترونية.

المحور الرابع: الجريمة المتعلقة بالدفع الالكتروني

المحور الخامس: سبل مكافحة الجريمة الالكترونية.

المحور الأول: الدراسات السابقة.

أولا: دراسة صغير يوسف، بعنوان الجريمة المرتكبة عبر الأنترنت، رسالة ماجستير، جامعة مولود معمري تيزي وزو، الجزائر،٢٠١٣.

تدور إشكالية هذه الدراسة حول تحديد خصوصية الجريمة المرتكبة عبر الانترنت مقارنة بالجرائم التقليدية والطرق الفعالة لمكافحتها، وقد توصل الباحث إلى ضرورة استحداث قوانين موضوعية وإجرائية تكون خاصة بها سواء على المستوى الوطني أو الدولي تتماشى مع العالم الافتراضي للشبكة الذي يختلف كل الاختلافات عن العالم التقليدي.

اختلفت هذه الدراسة عن موضوع الورقة البحثية من حيث أنها ركزت على الجوانب القانونية في مكافحة الجريمة الالكترونية، في حين ركزت الورقة البحثية على الجانب الاقتصادي وبالتحديد الجانب المالي. " الجرائم التي تمس الأموال"

ثانيا: دراسة دحمان صبايحية خديجة، جرائم السرقة والاحتيال عبر الانترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري، رسالة ماجستير، جامعة الجزائر، تخصص شريعة وقانون، سنة ٢٠١٣.

بحثت هذه الدراسة في التكييف الفقهي و القانوني لجرائم السرقة والاحتيال عبر الانترنت. وبالتالي فان الإخلاف بين الدراستين يكمن في أن الدراسة المذكورة ركزت على الجوانب الشرعية و القانونية، حيث تناولت نظرة الشريعة الإسلامية وموقفها من جرائم السرقة والاحتيال عبر الانترنت، كما تناولت التحقيق في الجريمة الالكترونية كإحدى السبل لمكافحتها. أما موضوع الورقة البحثية يختلف عن هذه الدراسة لكن كلاهما بحثا في ماهية الجريمة الالكترونية و سبل مكافحتها.

ثالثا: دراسة محمد عبد الله بن علي المنشاوي بعنوان: جرائم الانترنت في المجتمع السعودي، رسالة ماجستير مقدمة إلى كلية الدراسات العليا في العلوم الشرطية تخصص قيادة أمنية، سنة ٢٠٠٣.

من خلال الدراسة الميدانية توصل الباحث إلى وجود العديد من الجرائم و الممارسات غير الأخلاقية التي يرتكبها مستخدمي الانترنت في السعودية، وان الفئة الأكبر ارتكابا للجرائم الالكترونية هي فئة الشباب، لذلك أوصى الباحث المؤسسات الدينية بتكثيف البرامج الدينية الهادفة والبناءة لجذب مختلف فئات المجتمع وشغل أوقاتهم بما يفيد.

تختلف هذه الدراسة عن الدراسة الحالية في كونها دراسة ميدانية أشمل وأعم من الورقة البحثية الحالية، كما أن هذه الدراسة ركزت على النواحي الأمنية في حين ركزت الورقة البحثية على الجوانب الاقتصادية والمالية وهذا هو الاختلاف الجوهري بين الدراستين.

رابعا: دراسة نوال بنت علي محمد القيسي، بعنوان: بعض جرائم الانترنت الموجهة ضد مستخدمي الانترنت، رسالة ماجستير، جامعة الإمام محمد ابن سعود الإسلامية، كلية العلوم الاجتماعية.

تدور إشكالية هذه الدراسة حول تحديد حجم أهم جرائم الانترنت شيوعا بين مستخدمي الانترنت في المجتمع السعودي وخاصة فيما يتعلق بجرائم التحرش الجنسي، جرائم الاختراقات، جرائم القرصنة والجرائم المادية وجرائم الإرهاب الالكتروني مع تحديد أهم المشكلات التي تسببها لمستخدمي الانترنت في المجتمع السعودي.

تختلف هذه الدراسة عن الدراسة الحالية في كونها دراسة ميدانية خصت المجتمع السعودي كما أنها أشمل وأعم من الورقة البحثية الحالية، بحيث ركزت الورقة البحثية على الجوانب المالية أكثر من الجوانب الأخرى. في حين ركزت هذه الدراسة على النواحي الاجتماعية.

المحور الثاني: وسائل الدفع الالكترونية.

يقصد بالدفع الالكتروني استخدام التكنولوجيات الحديثة للاتصال كالانترنت، شبكة الهاتف، وذلك لتسوية الالتزامات.

أولا: وسائل الدفع الالكترونية، مفهوم وخصائص :

ويعرف الدفع الالكتروني على انه:" عملية تحويل الأموال هي في الأساس ثمن لسلعة أو خدمة بطريقة رقمية أي باستخدام أجهزة الكمبيوتر، وإرسال البيانات عبر خط تليفوني أو شبكة ما أو أي طريقة لإرسال البيانات". كما يعرف على انه:" مجموعة الأدوات والتحويلات الالكترونية التي تصدرها المصارف والمؤسسات كوسيلة دفع وتتمثل في البطاقات البنكية والنقود الالكترونية والشيكات الالكترونية والبطاقات الذكية."[1]

أما عن خصائصها فتتمثل في:[2]

- **الطبيعة الدولية في الدفع الالكتروني:** يعتبر الدفع الالكتروني وسيلة مقبولة في جميع الدول وفي جميع أنحاء العالم.
- **استخدام النقود الالكترونية:** تخصص لعملية الدفع الالكتروني نقود على شكل الكتروني، قد تكون على شكل شرائح، برامج أو أقراص ذاكرة.
- **البعد في تسوية المعاملات الالكترونية :** تسمح الانترنت بتسوية معاملات الدفع والتي تتسم بالبعد بين أطراف التعامل.
- **أسلوب الدفع:** يتم الدفع بطاقات مخصصة للشراء عبر الأنترنت أو من خلال البطاقات البنكية العادية.

يتم الدفع عبر شبكتين الأولى تختص فقط بأطراف التعامل و يلتزم وجود علاقات مالية وتجارية مسبقة بينهم وثانية عامة تتداولها الأفراد دون وجود روابط.

ثانيا: أنواع وسائل الدفع الالكترونية:

تأخذ وسائل الدفع الالكترونية عدة صور نذكر منها ما يلي:

١. البطاقات البنكية " بطاقات الائتمان ":

ويقصد بها البطاقات البلاستيكية والمغناطيسية التي تصدرها البنوك لعملائها للتعامل بها بدلا من حمل النقود، وأشهرها الفيزا (Visa)، و الماستر كارت (Master Card)، وأمريكان اكسبريس (Express American) وتقوم هذه البطاقات على مبدأ الدفع المسبق " pre-paiment" أي تكون هذه البطاقات مدفوعة القيمة المالية سلفا ومخزنة فيها، وبالتالي فهي عبارة عن وسيلة لتخزين النقد أي أنها بمثابة حافظات نقد الكترونية." port- monnaie electronique ". ويمكن استخدام هذه

---

[1] صراع كريمة، واقع وآفاق التجارة الالكترونية في الجزائر، مذكرة ماجستير في العلوم التجارية، جامعة وهران، ٢٠١٣/٢٠١٤، ص:٥٨.

[2] نفس المرجع السابق، ص:٥٩.

البطاقات للدفع عبر الانترنت وغيرها من الشبكات.كما يمكن استخدامها للدفع في نقاط البيع التقليدية – Point of sale p.o.s.[1]

وتتميز هاته البطاقات بالعديد من المزايا منها توفير الأمان لكل من المستهلك والتاجر وإمكانية القيام بالمشتريات الفورية والمدفوعات الآجلة باستخدام العملة المحلية سواء كانت القيمة منصرفة محليا أو خارجيا، وتسمح هاته البطاقات بمعرفة حاملها باستخدام المعالج الإلكتروني الموجود بداخلها ، كما تتميز بإمكانية شحنها عدة مرات.[2]

٢. البطاقات الذكية:

هي عبارة عن بطاقة بلاستيكية تحتوي على خلية إلكترونية يتم عليها تخزين جميع البيانات الخاصة بحاملها مثل الاسم، العنوان، المصرف المصدر، أسلوب الصرف، المبلغ المنصرف وتاريخه، وتاريخ حياة العميل المصرفية.

تسمح هذه البطاقة للعميل اختيار طريقة التعامل سواء كان ائتماني أو دفع فوري، وهو ما يجعلها بطاقة عالمية تستخدم على نطاق واسع في معظم الدول الأوروبية والأمريكية، كبطاقة المندكس "Mondex Card" و التي تتميز بالمزايا التالية:

.يمكن استخدامها كبطاقة ائتمانية أو بطاقة خصم فوري طبقا لرغبة العميل.

. سهولة إدارتها مصرفيا بحيث لا يمكن للعميل أن يستخدمها بقيمة أكثر من الرصيد المدون على الشريحة الالكترونية للبطاقة.

.أمان الاستخدام لوجود ضوابط أمنية محكمة في هذا النوع من البطاقات ذات الذاكرة الالكترونية .

. إمكانية التحويل من رصيد بطاقة إلى رصيد بطاقة أخرى من خلال آلات الصرف الذاتي أو أجهزة التليفون العادي أو المحمول.

.يمكن للعميل السحب من رصيد حسابه الجاري بالبنك وإضافة القيمة إلى رصيد البطاقة من خلال آلات الصرف الذاتي أو أجهزة التليفون العادي أو المحمول.[3]

٣. النقود الالكترونية:[4]

أطلق على هذا النوع مصطلح النقود الرقمية (Digital Money) أو العملة الرقمية (Digital Currency)، بينما استخدم البعض الآخر مصطلح النقدية الالكترونية (E – Cash) أو العملة الافتراضية.

---

[1]. أنظر في ذلك:

. نهى خالد عيسى الموسوي، إسراء خضير مظلوم ألشمري، النظام القانوني للنقود الالكترونية، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٢٢، العدد ٢، ٢٠١٤،ص:٢٧٠.

. رحيم حسين، هواري معراج، الصيرفة الالكترونية كمدخل لعصرنة المصارف الجزائرية، ملتقى المنظومة المصرفية الجزائرية والتحولات الاقتصادية . واقع وتحديات . يومي ١٤/١٥ ديسمبر ٢٠٠٤، ص:٣٢١

[2] عباس بلفاطمي، ورقة مقدمة إلى الملتقى الوطني حول المنظومة المصرفية في الألفية الثالثة : منافسة ، مخاطر وتقنيات المنعقد بـ: ٠٦ – ٠٧ جوان ٢٠٠٥ بجامعة جيجل ص:٧.

[3] مفتاح صالح، معارفي فريدة، البنوك الالكترونية، المؤتمر العلمي الخامس،نحو مناخ استثماري وأعمال مصرفية الكترونية، جامعة فيلادلفيا، عمان/ الأردن، ٤.٥ يوليو ٢٠٠٧، ص ص:١٠.١١.

[4] عباس بلفاطمي، مرجع سابق، ص:٥.

وتعرف النقود الالكترونية على أنها: " عبارة عن سلسلة من الأرقام التي تعبر عن قيم معينة تصدرها البنوك التقليدية أو الافتراضية لمودعيها ويحصل هؤلاء عليها في صورة نبضات كهرومغناطيسية على بطاقة ذكية أو على القرص الصلب ويستخدمها هؤلاء لتسوية معاملاتهم التي تتم الكترونيا".

أما صندوق النقد الدولي فيعرف على انه:" قيمة نقدية في شكل وحدات ائتمانية مخزنة في شكل الكتروني أو في ذاكرة الكترونية لصالح المستهلك".

ويمكن أن يتجسد النقد الإلكتروني في صورتين : حامل النقد الإلكتروني le e-cash ou porte monnaie électronique ، وهو عبارة عن بطاقة يخزن بداخلها قيمة نقدية، تسمح بإجراء مدفوعات المشتريات الصغيرة بين أطراف التبادل دون تدخل لوسيط . والنقد الشبكي la monnaie réseau الذي يتم تحويله عبر شبكات الاتصال العالمية (الإنترنت) للوفاء بقيمة المدفوعات، وهذا باستخدام برمجيات متخصصة des logiciels spécialisées مدمجة بأجهزة الكمبيوتر الخاصة.

وتتميز النقود الإلكترونية بالخصائص التالية :

. إمكانية تحويل القيمة إلى طرف آخر بواسطة تحويل المعلومات الرقمية وهذا يعكس إمكانية استخدام شهادة النقود الرقمية عدة مرات .

. التحويل يتم بواسطة الشبكات العالمية (الإنترنت) أو شبكات الاتصال اللاسلكية.

. إن الشخص الذي يستخدم النقود الإلكترونية هو مجهول المصدر anonymous وهذا لتوفير الأمن لعملية الدفع الإلكتروني .

. إن النقد الإلكتروني يتميز بقابليته للتجزئة وهذا لإجراء حتى العمليات صغيرة القيمة .

. يمكن استخدامها في أي وقت وفي أي مكان.

٤. المحافظ الالكترونية:

المحفظة الالكترونية عبارة عن تطبيق الكتروني يقوم على أساس ترتيب وتنظيم آلية جميع الحركات المالية، وتحتوي تلك المحفظة على جميع بيانات المستخدم لتلك البطاقة بصيغة مشفرة Encrypted ويتم تثبيتها على الكمبيوتر الشخصي أو تخزينها على أحد الأقراص المرنة أو أي أداة يمكن عن طريقها حفظ تلك البيانات واستخدامها للدفع عن طريق شبكة الانترنت في جميع حالات الشراء[1].

٥. الشيكات الالكترونية:

الشيك الالكتروني هو المكافئ الالكتروني للشيك الورقي التقليدي ، والشيك الالكتروني هو وثيقة الكترونية موثقة ومؤمنة تحتوي على البيانات الآتية : رقم الصك واسم الدافع ورقم حساب الدافع واسم المصرف واسم المستفيد والقيمة التي ستدفع ، ووحدة العملة المستعملة وتاريخ الصلاحية والتوقيع الالكتروني ولا يشترط أن يكون مكتوبا بخط اليد وموقعا بواسطة الشخص الذي يصدره . يرسل هذه الوثيقة مصدر الشيك إلى مستلم الشيك(حامله) ليعتمده ويقدمه للبنك الذي يعمل عبر الانترنت ، ليقوم البنك أولا بتحويل قيمة الشيك المالية إلى حساب حامل الصك وبعد ذلك يقوم بإلغاء الشيك وإعادته الكترونيا إلى مستلم الشيك ليكون دليلا على انه قد تم صرف الشيك فعلا ويمكن لمستلم الشيك أن يتأكد الكترونيا قد تم بالفعل تحويل المبلغ لحسابه، ويتعهد فيها البنك بسداد الشيكات التي يحررها العميل بشروط معينة، حيث يقوم البنك بفتح

[1] عايض المري، المحفظة الالكترونية، على الخط، http://www.dralmarri.com/show.asp ، تاريخ الاطلاع: ٢٠١٦/٠٣/٢٩، ص:١.

حساب وتحديد التوقيع الالكتروني للعميل، ويخطر كل من الطرفين بتمام إجراء المعاملة المصرفية ، أي خصم الرصيد من المشتري وإضافته لحساب البائع.[1]

٦.السفتجة الالكترونية:

هي عبارة عن محرر شكلي ثلاثي الأطراف معالج الكترونيا، بصورة كلية أو جزئيا، يتضمن أمرا من شخص يسمى الساحب إلى شخص آخر يسمى المسحوب عليه بأن يدفع مبلغا من النقود لشخص ثالث يسمى المستفيد لدى الاطلاع أو في تاريخ معين. ويمكن التمييز بين نوعين من السفتجة الالكترونية:

أ. **السفتجة الورقية أو المقترنة بكشف:" L.C.R. Papier"** ، تصدر في البداية في شكلها التقليدي على دعامة ورقية ثم يتم معالجتها الكترونيا عند تقديمها لدى البنك لتحصيلها أو بمناسبة تظهيرها لأي طرف آخر. ويكون لها شكلية الكترونية بواسطة بيانات تتداولعبر قنوات الاتصال بين حواسيب الأطراف المتعاملة بها.

ب. **السفتجة الممغنطة :" L.C.R. Magnetique "** تصدر من البداية على دعامة ممغنطة مستوفية لكافة البيانات اللازمة لصحتها الخاصة بالمستفيد، المسحوب والتوقيع الالكتروني. والواقع ان ذا النوع هو الذي يمثل قمة الاستفادة من التقنيات الالكترونية الحديثة، فتحرر وتتداول في كل مراحلها بالطرق الالكترونية.[2]

٧.التحويلات المالية الالكترونية:

يقصد بها عملية منح الصلاحية لبنك ما للقيام بحركات التحويلات المالية الدائنة والمدينة الكترونيا من حساب بنكي إلى حساب بنكي آخر أي أن عملية التحويل تتم الكترونيا عبر الهواتف وأجهزة الكمبيوتر وأجهزة المودم عوضا عن استخدام الأوراق.

أما عن كيفية تنفيذ عمليات التحويل المالي فتتم عن طريق دار الهاصة الآلية وهي شبكة تعود ملكيتها وأحقية تشغيلها إلى البنوك المشتركة بنظام التحويلات المالية الالكترونية.

وتتم عملية التحويل المالي الالكتروني بتوقيع العميل نموذجا معتمدا واحدا لصالح الجهة المستفيدة التاجر مثلا، ويتيح هذا النموذج اقتطاع القيمة المحددة من حساب العميل وفق ترتيب زمني معين _يوميا أو أسبوعيا أو شهريا- ويختلف نموذج التحويل المالي الالكتروني عن الشيك في أن صلاحيته تسري لأكثر من عملية تحويل واحدة، وفي العادة يتعامل البنك والعميل مع وسطاء وظيفتهم توفير البرمجيات اللازمة ويمكن إيجاد العديد منهم على الانترنت.

ويقوم العميل بإرسال التحويل المالي عن طريق المودم إلى الوسيط ويقوم هذا الأخير بتجميع التحويلات المالية وإرسالها إلى دار المقاصة المالية الآلية (ACH) التي بدورها ترسل نموذج التحويل المالي الالكتروني إلى بنك العميل ويقارن بنك العميل التحويل المالي-الوارد من دار المقاصة- برصيد العميل وفي حال عدم تغطية الرصيد لقيمة التحويل المالي يتم إرسال إشعار بعدم كفاية الرصيد إلى الوسيط ليقوم بدوره بإعادة الإشعار إلى العميل، أما إذا كان الرصيد كافيا لتغطية قيمة التحويل المالي فعندها يتم اقتطاع قيمة التحويل منه وتحويلها إلى حساب المستفيد (البنك أو التاجر) في وقت السداد المحدد بالنموذج .

أما إذا رغب التاجر في تنفيذ التحويلات المالية عبر دار المقاصة الآلية دون المرور بوسيط فعندها يتوجب على التاجر نفسه أن يشتري البرمجيات الخاصة التي تسمح بإجراء هذه العملية وتكون هذهالبرمجيات مؤمنة بكلمة مرور خاصة بالتاجر،

---

[١] نهى خالد عيسى الموسوي، إسراء خضير مظلوم ألشمري، مرجع سابق، ص:٢٧١.٢٧٢ .

[٢] واقد يوسف، النظام القانوني للدفع الالكتروني، مذكرة ماجستير، جامعة تيزي وزو، ٢٠١١ ،ص:٥٤.٥٥

وفي هذه الحالة يقوم العميل باعتماد نموذج الدفع مرفقا بشيك مصدق لصالح التاجر ثم يقوم التاجر بإرسال الاعتماد إلى دار المقاصة الآلية التي تقوم بدورها بإرسال الاعتماد إلى البنك لاقتطاع المبلغ من حساب العميل في الوقت المحدد وتحويله إلى حساب التاجر وفي هذه الحالة لا حاجة للتحقق من كفاية رصيد العميل لان الشيك المصدق يضمن ذلك .[1]

ثالثا : مزايا وعيوب وسائل الدفع الالكتروني

إن لوسائل الدفع الالكتروني مزايا وعيوب تتعلق بكل من حامل وسيلة الدفع الالكترونية ومصدرها وكذا التاجر الذي يتعامل بها، تتمثل في:[2]

ب.١ : مزايا وسائل الدفع الالكتروني:

تحقق وسائل الدفع الالكتروني العديد من المزايا تتمثل في:

١. **بالنسبة لحاملها:** سهولة ويسر استعمالها عكس النقود الورقية القابلة للتلف والضياع، فوسائل الدفع الالكترونية توفر لحاملها الأمان فما علية سوى حمل بطاقة الدفع. وتمكن حاملها فرصة الحصول على ائتمان المجاني، كما تمكنه ن اتمام صفقاته فور ذكر رقم البطاقة.

٢. **بالنسبة لمصدرها:** إن الفائدة التي تجنيها المصارف و المؤسسات المالية من إصدار البطاقات الالكترونية هي الفوائد والرسوم والغرامات من الأرباح فمثلا حقق بنك " city bank " أرباحا من حملة البطاقات الائتمانية لسنة١٩٩٥ قدرت بـ١ بليون دولار.

٣ . **بالنسبة للتاجر:** لطالما أن عبء متابعة ديون الزبائن يقع على عاتق البنوك و المؤسسات المصدرة فان البائع بعيد عن تحمل هذا العبء فهي تعد ضمان لحقوق البائع.

ب.٢ : عيوب وسائل الدفع الالكتروني:

أما عيوب وسائل الدفع الالكتروني فتتمثل في:

١. **بالنسبة لحاملها:** نظرا لزيادة الاقتراض و الإنفاق بما يفوت قدرة حامل البطاقة وكذا عدم تسديد ديونه في الوقت المحدد ينجم عنها سحب البطاقة منه ووضعه في القائمة السوداء.

2. **بالنسبة لمصدرها:** وهنا العيب ظهر في مدى سداد حاملي البطاقات الديون المترتبة عليهم وكذلك انه في حالة ضياعها فان البنك يتحمل النفقات.

3. **بالنسبة للتاجر:** عدم التزامه بالشروط مع البنك وارتكابه للمخالفات يلغي تعامله مع البنك مما يجعله في القائمة السوداء

المحور الثالث: الإطار النظري للجريمة الالكترونية.

تشير الإحصائيات المتعلقة بالجريمة الالكترونية انه؛ في بريطانيا وفي عام٢٠٠ هناك جريمة الكترونية تقع كل١٠ ثواني" ٣ مليون جريمة في السنة، أو٨ آلاف جريمة في اليوم" واكبر نسبة فيها تتعلق بالتحرش ٨٥٠ ألف حالة " ، بينما هناك٩٢ ألف حالة لسرقة الهوية أي الحصول على معلومات شخصية حول مستخدمي الانترنت، و١٤٤ ألف حالة لاختراق

[1] نهى خالد عيسى الموسوي، إسراء خضير مظلوم ألشمري، مرجع سابق، ص ص:٢٧٢.٢٧٣.

[2] صراع كريمة، مرجع سابق، ص:٧٦.

الحواسيب بهدف سرقة المعلومات أو التخريب، لا ٢٠ ألف حالة للحصول على الأموال من خلال الاحتيال للسطو على أرقام البطاقات الائتمانية. و تقول الإحصائيات أن شركات التأمين أن ٧٠ % من هذه الجرائم تستهدف الأفراد. والأطفال هم أكثر ضحايا الجرائم الالكترونية بحيث يستقبل ٨٠ % من الأطفال رسائل بريد دعائية كل يوم وبخاصة خلال فترات العطل، وبعض تلك الرسائل تتضمن محتوى لا ينبغي عليهم أن يطلعوا عليه في أي حال من الأحوال.[1]

أولا: مفهوم و خصائص الجريمة الالكترونية وتصنيف مرتكبوها :

يقول فان دير هلست ونيف " هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة ...وفي اغلب الأحيان تستخدم الافتراضية والحاسوب والالكترونية والرقمية وكلها تعكس فجوات مهمة في العريف". وتعريف الجرائم الالكترونية على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال.[2]

تتكون الجريمة الالكترونية أو الافتراضية من مقطعين هما الجريمة "crime" والالكترونية " cyber". ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات. أما الجريمة فهي السلوكيات والأفعال الخارجة عن القانون. والجرائم الالكترونية " هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت " غرف الدردشة، البريد الالكتروني ، والموبايل".[3]

تعرف أيضا على أنها:" هي جريمة ذات طابع مادي، تتمثل في كل فعل أو سلوك غير مشروع, من خلال استعمال الوسائط الإلكترونية مثل الحواسيب، أجهزة النقال ، شبكات الاتصالات الهاتفية، شبكات نقل المعلومات، شبكة الإنترنت، حيث تتسبب في تحميل أو إمكانية تحميل المجني عليه خسارة، وحصول أو إمكانية حصول مرتكبه على أي مكسب. تهدف هذه الجرائم إلى الوصول غير المشروع لبيانات سرية غير مسموح بالاطلاع عليها ونقلها ونسخها أو حذفها، أو تهديد وابتزاز الأشخاص والجهات المعنية بتلك المعلومات,أو تدمير بيانات وحواسيب الغير بواسطة فيروسات"[4].

وتتميز الجريمة الالكترونية عن غيرها من الجرائم التقليدية بما يلي:[5]

- استهدافها للكيانات المعنوية ذات قيمة مادية أو معنوية أو معنوية و مادية.
- التباعد الجغرافي بين مرتكب الجريمة والضحية.
- انخفاض حجم المخاطرة.
- سهولة ارتكاب الجريمة بعيداً عن أعين الرقابة الأمنية.
- سرعة ارتكاب الجريمة الإلكترونية.
- عدم وجود تقدير معين لحجم الضرر الناتج عنها.

---

[1] سمير سعدون مصطفى، محمود خضر سليمان، حسن كريم عبد الرحمن، الجريمة الالكترونية عبر الأنترنت أثرها وسبل مواجهتها، على الخط، *www.iasj.net/iasj?func=fulltext&aId=28384* ، تاريخ الاطلاع: ٢٠١٧/٠٢/٠١، ص:٤.

[2] ذياب موسى البدايني، الجرائم الالكترونية: المفهوم والأسباب، الجرائم المستحدثة في ظل المتغيرات و التحولات الإقليمية والدولية خلال الفترة ٢٠١٤/٠٩/٢،٤، كلية العلوم الإستراتيجية، عمان/ الأردن، ص:٠٣.

[3] نفس المرجع السابق، ص:٣.

[4] منى شاكر فراج العسبلي، مقال على الخط، http://kenanaonline.com/ ، تاريخ الاطلاع، ٢٠١٧/٠١/٠٨، ص:١.

[5] نفس المرجع السابق، ص:١.

•صعوبة تحديد المجرم ومعرفة مكانه نظراً لتفاوت الفئة العمرية لمرتكبي الجرائم الإلكترونية.

•قصور التشريعات والقوانين التي تدين هذا النوع من المجرمين .

•سهولة التخلص من الأدلة المدينة للمجرمين .

ونشير في هذا الإطار انه يمكن تصنيف المجرم الالكتروني في أربع مجموعات رئيسية وهي[1]:

.المجموعة الأولى : وهم الموظفون العاملون بمراكز الكمبيوتر وهم يمثلون الغالبية العظمى من مرتكبي الجرائم الإلكترونية، وذلك بحُكم سهولة اتصالهم بالحاسب ومعرفتهم بتفاصيله الفنية.

.المجموعة الثانية : وبتمثل في الموظفون المعارضون لمؤسساتهم أو شركاتهم والذين يستغلون معرفتهم بأنظمة الحاسب الآلي في شركاتهم وسيلة لإيقاع الضرر بهم عبر نشر البيانات أو استعمالها أو مسحها.

.المجموعة الثالثة : وتتمثل في فئة العابثين مثل الهاكرز (Hackers)أو الكراكز(crackers)، وهم الذين يستغلون الكمبيوتر من أجل التسلية في أمور غير قانونية وليس بغرض التخريب.

.المجموعة الرابعة: وهم الأفراد الذين يعملون في مجال الجريمة المُنظمة عبر استخدام الكمبيوتر.

ثانيا: الأفعال التي تشكل جرائم الانترنت:

لقد صنف مكتب الأمم المتحدة للمخدرات والجريمة، الأفعال التي قد تشكل الجرائم الالكترونية، وقد تم تنظيمها في ثلاث مجموعات تتمثل فيما يلي:[2]

أ. الأفعال ضد السرية والنزاهة وتوافر بيانات الحاسب أو النظم.

.الدخول غير المشروع لنظام الحاسوب.

.الدخول غير المشروع، اعتراض أو الاستيلاء على بيانات الحاسوب.

.الاستنتاج غير المشروع لبيانات الحاسوب أو نظامه.

.إنتاج أو توزيع أو امتلاك لأدوات إساءة استعمال الحاسوب.

.اختراق الخصوصية أو أساليب حماية البيانات.

ب. أفعال ذات الصلة بالحاسوب لمصالح شخصية أو مادية أو أذى.

.الاحتيال المتعلق بالحاسوب أو التزوير.

.جرائم الحاسوب ذات الصلة بالهوية.

.حقوق الطبع والنشر أو جرائم العلامة التجارية ذات الصلة بالحاسوب.

.إرسال أو السيطرة على إرسال البريد المزعج.

.الأعمال ذات الصلة بأجهزة الحاسوب الشخصية التي تسبب بالضرر.

. الإغراء أو استمالة الأطفال المتعلق بالحاسوب.

---

[1] الجريمة الإلكترونية في ظل تطور تكنولوجيا المعلومات، على الحط، http://kenanaonline.com ، تاريخ الاطلاع: ٢٠١٧.٠١.٢٤، ص:١

[2] ذياب موسى البدايني، مرجع سابق، ص: ٨.



ج. الأفعال ذات الصلة بمحتويات الحاسوب.

.الأفعال ذات الصلة بالحاسوب التي تنطوي على خطاب الكراهية.

.الإنتاج أو توزيع أو حيازة المواد الإباحية عن الأطفال المتعلقة بالحاسوب.

.الأعمال ذات الصلة بأجهزة الكمبيوتر في دعم جرائم الإرهاب.

ثالثا: مراحل و أسباب الجريمة الالكترونية.

مراحل حدوث الجريمة الالكترونية:

عادة ما تحدث الجريمة الإلكترونية عادة في إحدى ثلاث مراحل هي[1]:

.المرحلة الأولى : وتتمثل في مرحلة إدخال البيانات، فعلى سبيل المثال قيام المجرم الإلكتروني بتغيير أو تزوير البيانات مثل التسلل الإلكتروني إلى البيانات المتعلقة بفاتورة الهاتف قبل طبعها في شكلها النهائي بحيث يتمكن من حذف بعض المكالمات من الفاتورة قبل طباعتها وإرسالها، ومثل قيام أحد الطلاب بتغيير درجاته المسجلة على الكمبيوتر في مادة معينة أو تغيير معدله الفصلي أو العام.

المرحلة الثانية : وتتمثل في مرحلة تشغيل البيانات، مثل قيام المجرم الالكتروني بتغيير أو تعديل البرامج الجاهزة (soft wear) التي تقوم بتشغيل البيانات للوصول إلى نتائج محددة أو مقصودة بطريق غير شرعي من قبل الجاني، وكمثال لاستخدام برنامج معين لتقريب الأرقام المتعلقة بالعمولات البنكية على حساب أحد الأشخاص، أو تجميع الفروق بين الأرقام المقربة والأرقام الفعلية وإضافتها لحساب سرى آخر لنفس العميل .. وقد تبدو هذه الفروق بسيطة ولكنها ستكون كبيرة إذا تمت إضافتها خلال عدة سنوات.

.المرحلة الثالثة : مرحلة إخراج البيانات، ومثل ذلك سرقة بعض البيانات الإلكترونية أو المعلومات الآلية المتعلقة بمراقبة مخزون إحدى الشركات، أو إفشاء معلومة متعلقة بإحدى الشركات، أو إفشاء معلومة متعلقة بأحد العملاء.

أ. أسباب الجريمة الالكترونية:

هناك عدة أسباب أدت إلى ظهور و انتشار الجريمة الالكترونية نذكر منها ما يلي[2]:

ب.١ : الانبهار بالتقنية المعلوماتية.

مع ظهور التقنية المعلوماتية وانتشارها في المجتمعات الحديثة سواء تعلق الأمر بالمعلومات أو الحواسب، فإن الأمر في النهاية يؤدي إلى انبهار المجرمين بهذهالتقنية الحديثة، لذلك فإن هؤلاء ليسوا على جانب كبير من الخطورة، وإنما هم غالبا يفضلون تحقيق انتصارات تقنية ودون أن يتوفر لديهم أية نوايا سيئة.

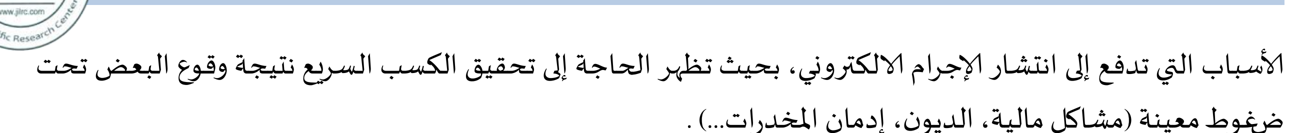
ب.٢ : الرغبة في تحقيق الثراء السريع.

قد تدفع الحاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الإطلاع على معلومات معينة أساسية وذات أهمية خاصة لمن يطلبها، ولذلك تتعدد الأساليب اللازمة للوصول إلى هذا الهدف المنشود، ولذلك فإن هذا السبب يعد من أكثر

---

[1] **الجريمة الإلكترونية في ظل تطور تكنولوجيا المعلومات، مرجع سابق، ص:١ .**

[2] الجرائم المرتبطة بتكنولوجيا المعلومات، على الخط، *salahgardafi.eb2a.com/wp-content*، *تاريخ الاطلاع:٢٤/٠١/٢٠١٧، ص:١ .*



الأسباب التي تدفع إلى انتشار الإجرام الالكتروني، بحيث تظهر الحاجة إلى تحقيق الكسب السريع نتيجة وقوع البعض تحت ضغوط معينة (مشاكل مالية، الديون، إدمان المخدرات...) .

ب.٣: الأسباب الشخصية.

يتأثر الإنسان في بعض الأحيان ببعض المؤثرات الخارجية التي تحيط به، ونتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، مع توفر هذه المؤتمرات، فإن الأمر يؤول في النهاية إلى ارتكابه للجريمة المعلوماتية، هذا وتتعدد المؤثرات التي تدفع الإنسان إلى اقتراف مثل هذا السلوك سواء كان ذلك بدافع اللهو أو الحقد أو الانتقام.

تبدأ الرغبة لدى الشباب نحو العبث بالأنظمة المعلوماتية من أجل ممارسة هواية اللعب، أو تعود إلى وجود ميل زائد لدى البعض بأن الاعتقاد بأن كل شيء يرجع إليهم، إذن تلك تمثل آفة نفسية تصيبهم ويتفاخرون بما قاموا به من جرائم، ليظهروا تفوقهم على الأنظمة المعلوماتية، وقد يكون الدافع نحو ارتكاب الجريمة المعلوماتية هو عامل الانتقام، وذلك عندما يتم فصل العامل من عمله فإن ذلك من شأنه أن يهيئ له المناخ لجريمته، كأن يدمر البرامج المعلوماتية بالفيروسات عن طريق زرعها.

المحور الرابع: الجريمة المتعلقة بالدفع الالكتروني:

سنحاول في هذا الاطار التعرف على حجم جرائم الدفع الالكترونية من خلال بعض الإحصائيات، كما سنتطرق إلى بعض الوسائل المستخدمة في اختلاس الأموال عبر الإنترنت.

أولا: بعض الإحصائيات المتعلقة بجريمة الدفع الالكتروني:[1]

تشير مجلة لوس انجيلوس تايمز في عددها الصادر في ٢٢ مارس عام 2000 إلى أن خسارة الشركات الأمريكية من جراء الممارسات التي تتعرض لها و التي تندرج تحت بند الجريمة الالكترونية بحوالي ١٠ مليار دولار سنويا، و للتأكيد على جانب قد تغفله الكثير من مؤسسات الأعمال فان نسبة ٦٢% من تلك الجرائم تحدث من خارج المؤسسة و عن طريق شبكة الانترنت بينما تشكل النسبة الباقية (٣٨ %) من تلك الخسائر من ممارسات تحدث من داخل المؤسسات ذاتها.
ذكر أيضا تقرير مكتب التحقيقات الفيدرالية الأمريكية التطور السنوي للخسائر المادية للشركات الأمريكية من الجرائم الالكترونية في الأعوام من ٢٠٠١ إلى ٢٠٠٣ الذي اظهر جنوح اغلب الجرائم إلى الانخفاض في حجم الخسائر السنوية ماعدا جريمة تعطيل العمل للأنظمة و الذي تضاعف حجم الخسائر المادية الناجمة منها من حوالي ١٨ مليون دولار عام ٢٠٠٢ إلى ما يقارب الـ ٦٥ مليون دولار عام ٢٠٠٣.

أشارت منظمة الـ بى اس ايه (BSA) العالمية Business Software Alliance في تقريرها السنوي الثامن يونيو ٢٠٠٣ إلى أن خسائر شركات البرمجيات وصلت إلى ١٣.٠ مليار دولار امريكى في عام ٢٠٠٢ و يشير التقرير أيضا إلى أن أكثر دول العالم في نسخ البرامج و العمل بنسخ غير مرخصة هي فيتنام حيث يصل نسبة النسخ غير المرخصة إلى حوالي ٩٧ % من إجمالي البرامج المستخدمة تليها دولة الصين بنسبة ٩٤ % ثم اندونيسيا بنسبة ٨٩ %. ويشير نفس التقرير إلى تحسن نسب القرصنة في مصر من ٨٦ % عام ١٩٩٤ إلى حوالي 52% عام ٢٠٠٢.

---

[1] فؤاد جمال، الجرائم المعلوماتية، على الخط، bleidaktaoua.blogspot.com/2012/10/blog-post_7399.html، *تاريخ: الاطلاع: ٢٠١٧/٠٢/٠١ . ص: ١ .*

أما في الولايات المتحدة فقد بدأت رابطة شركات الاسطوانات الاميريكية معركتها ضد المواقع الالكترونية التي تقدم خدمات تبادل الملفات وتحميل الأغاني بالمجاني على أجهزة الكمبيوتر عام١٩٩٩ و ذلك بعد انخفاض مبيعات الاسطوانات بنحو٣١ % بسبب النقل و النسخ عبر الانترنت و قد تحقق للرابطة بالفعل إغلاق احد أشهر مواقع بث الأغاني والذي يدعى Napster و مازالت العديد من القضايا مرفوعة من قبل الرابطة ضد شركات بث الأغاني أو خوادم التبادل بين المستخدمين بل ووصل الأمر إلى رفع العديد من القضايا على الأطفال والمراهقين مستخدمي تلك البرامج للاستماع و الحفظ و التبادل للمصنفات .

ثانيا: أساليب الجرائم الالكترونية المتعلقة بالدفع:

هناك عدة طرق يستطيع من خلالها المجرم الالكترونية سرقة أموال الغير من خلال الشبكة الالكترونية:

١ - : الوسائل الفنية للتحويل الإلكتروني للأموال:[1]

يتم التحويل غير المشروع للأموال بعدة وسائل يصعب حصرها لسرعة وتيرة التطور في هذا المجال لكن يمكن الإشارة إلى أكثرها انتشاراً.

أ: استخدام برامج معده خصيصا لتنفيذ الاختلاس :

من بين هذه الوسائل هو تصميم برامج معينة تهدف إلى إجراء عمليات التحويل الآلي من حساب إلى أخر سواء كان ذلك من المصرف نفسه أو من حساب أخر في مصرف أخر على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج، كما توجد برامج أخرى تقوم بخصم مبلغ ضئيلة من حسابات الفوائد على الودائع المصرفية بإغفال الكسور العشرية بحيث يتحول الفارق مباشرة إلى حساب الجاني لأنها برامج تعتمد على التكرار الآلي لمعالجة معينة ومما يؤدي إلى صعوبة اكتشاف هذه الطريقة رغم ضخامة المبلغ هو أن هذه الاستقطاعات تتم على مستوى ألاف الأرصدة في وقت واحد مع ضآلة المبلغ المخصوم من كل حساب على حده بحيث يصعب أن ينتبه إليه العميل.

ومن أشهر جرائم سرقة الأموال و التي جرت أحداثها في إمارة دبي بدولة الإمارات العربية المتحدة في أواخر عام٢٠٠ ما قام به مهندس حاسبات أسيوي يبلغ من العمر ٣١ عاما و تم نشر وقائع الجريمة في ابريل من عام٢٠٠٣ حيث قام بعمل العديد من السرقات المالية لحسابات عملاء في١٣ بنكاً محلياً و عالمياً حيث قام باختلاس الأموال من الحسابات الشخصية و تحويل تلك الأموال إلى حسابات وهمية قام هو بتخليقها كما قام أيضا بشراء العديد من السلع و الخدمات عبر شبكة الانترنت مستخدماً بيانات بطاقات الائتمان والحسابات الشخصية لعدد كبير من الضحايا. كل ذلك تم من خلال الدخول للشبكة من خلال إحدى مقاهي الانترنت العامة المنتشرة في دبي و قد بلغت قيمة الاختلاسات حوالي٣٠ ألف درهم من البنوك المحلية بالإمارات فقط. جريمة أخرى جرت وقائعها لأحد فروع سيتي بنك بالولايات المتحدة الأمريكية عام١٩٩٤ وكان بطلها مواطن روسي الجنسية الذي استطاع الاستيلاء على ما يقارب٤٠ ألف دولار أمريكي.

[1] رحاب عميش، الجريمة المعلوماتية، على الخط، *iefpedia.com/arab/wp-content/uploads/2010/04*، *تاريخ الاطلاع: ٢٠١٧/٠١/٢٤*، ص ص:١٠-١٢.



ب: التحويل المباشر للأرصدة:

يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور ، أشهرها قيام احد خبراء الحاسب الآلي في الولايات المتحدة باختراق النظام المعلوماتي لأحد المصارف وقيامه بتحويل١٢ مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط وعادة ما يتم ذلك أيضا عن طريق إدخال معلومات مزيفة وخلق حسابات و مرتبات وهمية وتحويلها إلى حساب الجاني ، ويمكن أن يتم التحويل المباشر أيضا عن طريق التقاط الإشعاعات الصادرة عن الجهاز إذا كان النظام المعلوماتي متصلا بشبكة تعمل عن طريق الأقمار الصناعية، فهناك بعض الأنظمة التي تستخدم طابعات سريعة تصدر أثناء تشغيلها إشعاعات اليكترومغناطيسية ثبت أنه من الممكن اعتراضها والتقاطها أثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز وإعادة بثها مرة أخرى بعد تحويرها.

ج- التلاعب بالبطاقات المالية :

لقد ظهرت أولى هذا النوع من الاحتيال بالتقاط الأرقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي للنقود إلى أن ظهرت الصرافة الآلية Electronic Banking والنقود المالية digital Cash.

أما جرائم الاعتداء على هذه البطاقات فتتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها أو بعد سرقة الأرقام السرية الخاصة بها وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن أن تسجل عليها أرقام هذه البطاقات.

ومن أشهر القضايا التي حدثت في مصر في بدايات عام٢٠٠ وهى استغلال أرقام بطاقات الائتمان الشخصية للشراء عبر الانترنت و قد قامت إدارة المعلومات و التوثيق و جرائم الحاسب الآلي بوزارة الداخلية بضبط الجاني و تقديمه للمحاكمة.

د. جرائم الاعتداء على أجهزة الصرف الآلي للنقود :

تثور هذه المشكلة في حالة استخدام الجهاز لصرف ما يتجاوز الرصيد الفعلي إذا تم ذلك بواسطة العميل صاحب البطاقة فالمسألة هنا لا تعدو أن تكون مسألة مديونية بين المؤسسة المالية والعميل لان الاستيلاء على المبلغ لم يتم دون رضاء المؤسسة المالية طالما أن هذه الأخيرة تعلم بأن الجهاز غير مرتبط بسقف حساب العميل حتى لا يتجاوزه.

ه: جرائم الاستيلاء على النقود الالكترونية :

هي مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الالكترونية أن تحل فعليا محل تبادل العملات النقدية، ومن هذه البطاقات ما يعمل عن طريق إدخالها إلى المركز الخاص بالمعاملة المصرفية لدى البائع أو الدائن حيث تم انتقال البيانات الاسمية من البطاقة إلى الجهاز الطرفي للبائع تحول عليه نتائج عمليات البيع والشراء إلى البنك الخاص بالبائع. ويعتبر الاستيلاء على هذا النوع من النقود من الجرائم الالكترونية التي تمس الدفع الالكتروني.

٢ : غسيل الأموال عبر الأنترنت:

لقد أعطت شبكة الإنترنيت عدة مميزات لمن يقومون بعمليات غسيل الأموال منها السرعة الشديدة، وتخطي الحواجز الحدودية بين الدول، وتفادي القوانين التي قد تضعها بعض الدول وتعيق نشاطهم وكذلك تشفير عملياتهم مما يعطيها قدرا أكبر من السرية. وأيضا كان انتشار التجارة الإلكترونية عبر شبكة الأنترنت خير المعين لهؤلاء القائمين على عمليات غسيل الأموال كالتجارة الإلكترونية وانتشارها عبر أنحاء العالم، قد ساعد كثيرا في عمليات غسيل الأموال نظرا لسرعة الاتفاق على الصفقات وإتمامها من خلاله دون أن تكون في معظم الأحيان تحت رقابة قانونية صارمة بل إنه في حالة وجود رقابة قانونية

يكون من الممكن تفادي تلك الرقابة وإتمام تلك الصفقات عبر الاتفاق على خطوات وترتيبات تنفيذها عبر الأنترنت وبطريقة تشفير معقدة لا يمكن حلها وبالتالي لا يمكن من خلالها معرفة كيفية إتمام تلك الصفحات.[1]

المحور الخامس: سبل مكافحة جرائم الدفع الالكتروني.

لقد أصبحت الأنترنت أداة أساسية للتعاملات المالية التي تجري بين الزبون ومنظمات الأعمال ومتاجرها الالكترونية، لذلك فان سرية وأمن المعلومات. التي يجري تبادلها عند إبرام الصفقات التجارية الالكترونية خصوصا عندما يتعلق الأمر بأسرار العمل أو بقضايا مالية. أصبحت قضية مهمة وضرورية لنجاح التجارة الالكترونية والدفع الالكتروني.

أولا: الطرق الوقائية للتصدي للجريمة الالكترونية:

ينبغي على كل متعامل مع الشبكة الالكترونية أن يحتاط مسبقا لكي لا يقع ضحية هذا النوع من الجرائم ويكون ذلك من خلال تتبع النقاط التالية: [2]

- توعية الناس لمفهوم الجريمة الإلكترونية وأنه الخطر القادم ويجب مواجهته والحرص على ألا يقعوا ضحية له.
- ضرورة التأكد من العناوين الإلكترونية التي تتطلب معلومات سرية خاصة كبطاقة ائتمانية أو حساب البنكي.
- عدم الإفصاح عن كلمة السر لأي شخص والحرص على تحديثها بشكل دوري واختيار كلمات سر غير مألوفة.
- عدم حفظ الصور الشخصية في الكمبيوتر.
- عدم تنزيل أي ملف أو برنامج من مصادر غير معروفة.
- عدم إيقاف برامج مكافحة الفيروسات والجدار الناري.
- الحرص على تحديث أنظمة الحماية.
- تكوين منظمة لمكافحة الجريمة الإلكترونية.
- إبلاغ الجهات المختصة في حال التعرض لجريمة إلكترونية.
- وضع أنظمة تشريعية متطورة لتنظيم البيئة القانونية والتنظيمية والتي تخدم أمن تقنيات ونظم المعلومات.
- تتبع تطورات الجريمة الإلكترونية وتطوير الوسائل والأجهزة والتشريعات لمكافحته.
- تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الالكترونية وبرمجيات الفيروسات وبرامج التجسس.

ثانيا: أهم الوسائل والأنظمة المستخدمة لتأمين الدفع الالكتروني.

من الوسائل المستخدمة في تأمين التعاملات المالية الالكترونية نذكر ما يلي:[3]

---

[1] الجرائم المرتبطة بتكنولوجيا المعلومات، مرجع سابق، ص:٤٧.

[2] منى شاكر فراج العسبلي، مرجع سابق، ص:١.

[3] انظر في ذلك:

. صراع كريمة، مرجع سايق، ص ص٧٧.٨٣.

. أمن التجارة الالكترونية، على الخط، http://www.abahe.co.uk/information-technology-enc، تاريخ الاطلاع:٢٣.٠١.٢٠١٧، ص:١.

١. تقنية طبقة الفتحات الآمنة (SSL) :

هو برنامج به بروتوكول تشفير متخصص لنقل البيانات و المعلومات المشفرة بين جهازين عبر شبكة الإنترنت بطريقة أمنه بحيث لا يمكن لأحد من الناس قراءتها غير المرسل و المستقبل وفي نفس الوقت تكون قوة التشفير فيها قوية و يصعب فكها,وهي تختلف عن بقية طرق التشفير في شئ واحد ألا وهو عدم الطلب من مرسل البيانات اتخاذ أي خطوات لتشفير المعلومات المراد حمايتها وكل الذي يفعله المستخدم هو التأكد من استخدام هذا البروتوكول بالقوة المطلوبة.

يقوم هذا البرنامج بربط المتصفح الموجود على جهاز المستخدم (المشتري) بجهاز الخادم الخاص بالموقع المراد الشراء منه وهذا طبعا إذا كان الخادم مزود بهذه التقنية أساسا، و يقوم هذا البرنامج بتشفير أي معلومة صادرة من ذلك المتصفح وصولاً إلى جهاز الخادم الخاص بالموقع باستخدام بروتوكول التحكم بالإرسال وبروتوكول الإنترنت وهو ما يعرف بـ TCP/IP و لقد سميت بالطبقة الآمنة لأن هذا البرنامج يعمل كطبقة وسيطه تربط بين بروتوكول التحكم بالنقل و بروتوكول HTTP:// (HyperText Transfer Protocol)

٢. الحركات المالية الآمنة (SET)

يشبه هذا البرنامج إلى حد كبير بروتوكول الطبقات الأمنية في استناده إلى التشفير والتوقيعات الرقمية ويستخدم هذا البروتوكول برمجيات تدعى برمجيات المحفظة الالكترونية وهذه المحفظة تحتوي على رقم حامل البطاقة والشهادة الرقمية التابعة له، كذلك فانه يحصل على شهادة رقمية صادرة عن احد البنوك الذي يعتمدها. وعند إجراء الحركات المالية عبر الانترنت فان كلا من التاجر وحامل البطاقة الشهادة الرقمية لكل منهما مما يتيح التحقق من هوية الأخر وإثناء إجراء الحركات المالية لا يمكن مشاهدة رقم البطاقة الائتمانية لهذا الزبون باستخدام هذا البروتوكول حيث ترسل الصيغ المشفرة لهذا الرقم إلى مصدر البطاقة الموافقة على إجراء الحركة المالية مع التاجر. كما يمكن للتاجر تلقي الدفعات من الزبائن دون شهادة بروتوكولSET . في هذه الحالة ما على التاجر إلا استخدام شهادة SET الخاصة به لتوثيق الحركات المالية مع البنك أو معالج الحركات المالية الذي يتعامل معه.

٣. التشفير:

هو تحويل المعلومات إلى شفرات غير مفهومة " دون معنى" لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات. وبعبارة أخرى هو " تحويل النصوص العادية إلى نصوص مشفرة وذلك باستخدام مفاتيح وهذه المفاتيح تستند إلى صيغ رياضية معقدة " خوارزميات" وتعتمد قوة و فعالية التشفير على أساسين: الخوارزمية وطول المفتاح " المقدار بـ Bits".

أما فك التشفير فهو عملية إعادة تحويل البيانات إلى صيغتها الأصلية وذلك باستخدام المفتاح المناسب لفك الشفرة. ونميز في التشفير بين نوعين:

أ. التشفير المتماثل: في هذا النوع يستطيع كل من المرسل والمستقبل من فك شفرة المعلومات بنفس المفتاح السري للثن هذا النوع يطرح مشكلة الأمان وعدم التحقق من الهوية. لذلك تراجع استخدام هذا النوع من التشفير.

ب. التشفير اللامتماثل: في هذا النوع من التشفير يستلزم استخدام نوعين من المفاتيح الخاص والعام. فالمفتاح الخاص يكون معرف من جهة واحدة فقط وهو الشخص القار على تشفير المعلومات و فك شفرتها.أما المفتاح العام فيكون معرفا لدى أكثر ن جهة ويستطيع فك شفرة الرسالة التي شفرها المفتاح الخاص. إذن المبدأ الذي تقوم عليه هذا النوع من التشفير وهو أن المعلومة التي يتم تشفيرها من احد المفاتيح لا يتم فك شفرتها إلا من طرف المفتاح الآخر.

نظام التشفير باستخدام المفاتيح العامة يدعى بنظام RSA يعتبر أبطأ مقارنة مع نظام التشفير المتماثل و أكثر أمانا، لكنه ليس عصيا على الاختراق، لذلك تم تطوير نظام PGP وهو نظام مطور محسن للنظام السابق. ولا يزال هذا النظام منيعا عن الاختراق حتى يومنا هذا فهو يستخدم مفتاحا بطول ١٢٨ Bits إضافة إلى استخدامه البصمة الالكترونية.

٤. البصمة الالكترونية:

هي بصمة رقمية يتم اشتقاقها وفق خوارزميات معينة تدعى دوال أو اقترانات التمويه وتقوم هذه الخوارزميات بتطبيق حسابات رياضية على الرسالة لتوليد بصمة "رسالة صغيرة" تمثل ملف كامل أو رسالة " سلسلة كبيرة " و تتكون البصمة الالكترونية للرسالة من بيانات لها طول ثابت " بين١٢٨ و١٦ Bits" تؤخذ من الرسالة المحولة ذات الطول المتغير وهذه البصمة تميز الرسالة الأصلية والتعرف عليها بدقة.أما اذا تم التغيير ولو بمقدار Bits في الرسالة. فسيؤدي هذا إلى بصمة أخرى مختلفة تماما. وتتميز البصمات عن بعضها البعض بحسب المفاتيح الخاصة التي أنشأتها التي لا يمكن فك شفرتها إلا بالمفتاح العام.

وتجدر الإشارة أن استخدام خوارزمية البصمة الالكترونية أسرع من عملية التشفير اللاتماثل لهذا فان البصمة الالكترونية تستخدم كثيرا في إنشاء التواقيع الرقمية.

٥. التوقيع الرقمي:

يستخدم من اجل التأكد من أن الرسالة من مصدرها دون التعرض لأي تغيير أثناء عملية النقل، بحيث يستخدم المرسل المفتاح الخاص لتوقيع الوثيقة الكترونيا أما المستقبل فيتحقق من صحة التوقيع عن طريق المفتاح العام. ويمكن دمج بين البصمة الالكترونية والمفتاح العام بحيث تموه الرسالة أولا لإنشاء بصمة الكترونية. ثم تشفر البصمة الالكترونية باستخدام المفتاح الخاص للمالك مما ينتج عنه توقيع رقمي يلحق بالوثيقة المرسلة وللتأكد من صحة التوقيع ستخدم المستقبل المفتاح العام المناسب لفك شفرة التوقيع.

وتقوم شركة سايبر سيف بتطوير شكل آخر من التوقيع الرقمي وهو بطاقات ذكية بحجم بطاقات الائتمان التي تبرمج بشفرة المستخدم الخاصة به.

٦. الشهادات الرقمية:

هي عبارة عن وثائق الكترونية تثبت هوية المستخدمين عبر شبكة الانترنت ويتولى إصدار هذه الشهادات جهة موثوق فيها تسمى سلطة إصدار الشهادات، تحتوي كل شهادة رقمية يتم إصدارها على معلومات مهمة تتعلق بمالكها وبالسلطة التي أصدرت هذه الشهادة مثل:

.اسم حامل الشهادة.

.المفتاح العام لحامل الشهادة.

.اسم سلطة إصدار الشهادة الرقمية

.رقم متسلسل.

.تاريخ الإصدار.

.مدة صلاحية الشهادة.

ومثال على ذلك المؤسسة العالمية المانحة للشهادات الرقمية عبر أطراف معتمدة وهي تصدر ثلاث أنواع من الشهادات الرقمية:

.شهادات التعريف الرقمية على مستوى الأفراد.

.شهادات التعريف الرقمية على مستوى مزودات " خادم" الويب المستخدمة في مواقع التجارة الالكترونية.

.شهادات التوقيع الرقمية التي تستخدم في توقيع الرسائل الالكترونية.

٧. الجدران النارية:

هو برنامج تطبيقي يقوم بحماية البيانات المخزنة على الخادم من أي هجوم أو اختراق، ففي حالة تعليمات أو أوامر غير مسموح بها يعلم هذا البرنامج المستخدم عن حدوث اختراق للمعلومات. كذلك في حالة دخول المستخدم إلى بيانات أو معطيات عبر الانترنت، فان هذا البرنامج ينذر المستخدم بأن هذه المعطيات أو هذا الموقع غير آمن وبالتالي سوف ستعرض إلى اختراق.

الخلاصة و التوصيات:

أدى ظهور الإنترنت إلى إيجاد نوع جديد من الجرائم يعرف بالجريمة الإلكترونية، وقد انتشرت هذه الجرائم بشكل واسع بسبب خواصها التي تميزها عن الجريمة التقليدية . بحيث يتعرض ضحايا هذه الجرائم لتعطيل وتدمير لمخازن المعلومات الخاصة بهم وسرقة أموالهم والتهديد والابتزاز . مما يؤثر وبشكل سيئ على الاقتصاد، لذلك تسعى العديد من الدول جاهدة لإيجاد طرق وأساليب للحد من هذه الجرائم.

ولقد تناولت هذه الورقة البحثية الجرائم الالكترونية المتعلقة بالدفع الالكتروني، بحيث تعرفنا في المحور الأول للدراسة على وسائل الدفع الالكتروني، أما في المحور الثاني فقد تناولنا الإطار النظري للجريمة الالكترونية، ثم تعرفنا على الجرائم التي تمس جانب الأموال، واهم الطرق التي يستخدمها المجرم الالكتروني للسطو على أموال الغير، وفي الأخير تعرفنا على الأهم الأساليب المستخدمة لمكافحة هذا النوع من الجرائم.

وبناءا على الفرضيات المذكورة سابقا، تم التوصل إلى:

• صحة الفرضية الأولى والقائلة أن الجرائم الالكترونية هي تلك الجرائم التي ترتكب عن طريق استخدام شبكة الانترنت، وقد تم التأكد من صحة الفرضية من خلال تناول الإطار النظري للجريمة الالكترونية حيث تم التطرق إلى أهم التعاريف المتعلقة بالجريمة الالكتروني.

• صحة الفرضية الثانية والقائلة بأن هناك العديد من الشركات في مختلف دول العالم تتعرض إلى خسائر اقتصادية ضخمة نتيجة تعرضها للجريمة الالكترونية، وذلك من خلال ذكر بعض الإحصائيات المتعلقة بالجريمة الالكترونية .

• صحة الفرضية الثالثة والقائلة بأن أول خطوة للقضاء على هذا النوع من الجرائم هو الوقاية منها من خلال التعريف بها وتوعية المجتمع بمخاطرها، وقد ثبت ذلك من خلال تناول الطرق الوقائية من الجريمة الالكترونية، ومن بينها التعرف على هذه الجرائم وتوعية المجتمع بها وكذا التأمين الالكتروني لوسائل الدفع الالكترونية لتفادي هذا النوع من الجرائم.

وبناءا على ما سبق تم التوصل إلى التوصيات التالية:

. حث الجامعات و المراكز البحثية العربية للبحث والدراسة في الجرائم الالكترونية، من خلال عقد المزيد من الندوات العلمية و المؤتمرات حول الجريمة الالكترونية. ومحاولة إنشاء شهادات متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة تلك الجرائم.

.تخصيص دورات تدريبية مكثفة، للقضاة و العاملين في مجال مكافحة الجريمة الالكترونية.لرفع مستوى الكفاءة لديهم في استخدام التقنية المعلوماتية.

. على الدول العربية المضي في عقد اتفاقات دولية إقليمية و عربية للتعاون على مكافحة الجرائم المعلوماتية و التنسيق والتعاون فيما بينها لإنشاء مجموعات عمل عربية لدراسة ووضع استراتيجيات وسياسات وإجراءات تنفيذية لمواجهة مثل هذه الجرائم.

.حث جامعة الدول العربية لإصدار قانون نموذجي موحد لمكافحة الجرائم الالكترونية.

المراجع:

. أمن التجارة الالكترونية، على الخط، http://www.abahe.co.uk/information-technology-enc، تاريخ الاطلاع:٢٠١٧.٠١.٢٣.

. الجرائم المرتبطة بتكنولوجيا المعلومات، على الخط، *salahgardafi.eb2a.com/wp-content، تاريخ الاطلاع:٢٤/٠١/٢٠١٧.*

. الجريمة الإلكترونية في ظل تطور تكنولوجيا المعلومات، على الخط، http://kenanaonline.com ، تاريخ الاطلاع: ٢٠١٧.٠١.٢٤.

. ذياب موسى البدايني، الجرائم الالكترونية: المفهوم والأسباب، الجرائم المستحدثة في ظل المتغيرات و التحولات الإقليمية والدولية خلال الفترة ٢٠١٤/٠٩/٢،٤، كلية العلوم الإستراتيجية، عمان/الأردن.

. رحاب عميش، الجريمة المعلوماتية، على الخط ، *iefpedia.com/arab/wp-content/uploads/2010/04، تاريخ الاطلاع: ٢٤/٠١/٢٠١٧.*

. رحيم حسين، هواري معراج، الصيرفة الالكترونية كمدخل لعصرنة المصارف الجزائرية، ملتقى المنظومة المصرفية الجزائرية والتحولات الاقتصادية . واقع وتحديات . يومي ١٤/١٥ ديسمبر ٢٠٠٤.

. سمير سعدون مصطفى، محمود خضر سليمان، حسن كريم عبد الرحمن، الجريمة الالكترونية عبر الأنترنت أثرها وسبل مواجهتها، على الخط، *www.iasj.**net**/iasj?func=fulltext&aId=28384* ، تاريخ الاطلاع: ٢٠١٧/٠٢/٠١.

. صراع كريمة، واقع وآفاق التجارة الالكترونية في الجزائر، مذكرة ماجستير في العلوم التجارية، جامعة وهران، ٢٠١٤/٢٠١٣.

. عايض المري، المحفظة الالكترونية، على الخط، http://www.dralmarri.com/show.asp ، تاريخ الاطلاع : ٢٠١٦/٠٣/٢٩.

عباس بلفاطمي، ورقة مقدمة إلى الملتقى الوطني حول المنظومة المصرفية في الألفية الثالثة : منافسة ، مخاطر وتقنيات المنعقد بـ: ٠٦ – ٠٧ جوان ٢٠٠٥ بجامعة جيجل.

. على الخط.، http://www.djelfa.info/vb/archive/index ، تاريخ الاطلاع: ٢٠١٦/٠٣/٢٩.

. فؤاد جمال، الجرائم المعلوماتية، على الخط، *bleidaktaoua.blogspot.com/2012/10/blog-post_7399.html_* ، *تاريخ الاطلاع: ٢٠١٧/٠٢/٠١* .

. مفتاح صالح، معارفي فريدة، البنوك الالكترونية، المؤتمر العلمي الخامس،نحو مناخ استثماري وأعمال مصرفية الكترونية، جامعة فيلادلفيا، عمان/الأردن، ٤.٥ يوليو ٢٠٠٧.

. منى شاكر فراج العسبلي، مقال على الخط، http://kenanaonline.com/ ، تاريخ الاطلاع، ٢٠١٧/٠١/٠٨.

. نهى خالد عيسى الموسوي، إسراء خضير مظلوم ألشمري، النظام القانوني للنقود الالكترونية، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٢٢، العدد ٢، ٢٠١٤.

. واقد يوسف، النظام القانوني للدفع الالكتروني، مذكرة ماجستير، جامعة تيزي وزو، ٢٠١١.

الجريمة الالكترونية الممارسة ضد المرأة على صفحات الانترنت وطرق محاربتها.

د. بن غذ فة شريفة و د. القص صليحة جامعة سطيف٢ الجزائر

الملخص:

لطالما تعرضت المرأة إلى الكثير من الاضطهاد الذي لم يختفي رغم كل التطور والتقدم، والمتمثل في القرية الالكترونية التي لم تعد تختلف عن القرية القديمة من حيث الزمن. حيث أن صورة المرأة مازالت سلعة يتاجر بها كل من سولت له نفسه ذلك وعِرض المرأة العربية لم يختلف كثيرا في اضطهاده على شبكات الانترنت عن سابق الأزمان، حيث أصبحت الحسابات الالكترونية الخاصة بالمرأة حسابات مشاع لكل قرصان أو مجرم الكتروني له نزوات عدوانية ضدها سواء كانت مكبوتة أو معلنة.

كما أن التهديدات المتنوعة على مختلف صفحات الويب لا تتوقف، بل في تزايد مستمر. حتى الحياة الخاصة للمرأة وحياتها الزوجية والمهنية أصبحت محل تهديد دائم. فكم من امرأة طلقت وطردت من وظيفتها أو بيتها بسبب هذه التحرشات التكنولوجية. ورغم أن محاولات التصدي لمثل هذه التحرشات والتهديدات والجرائم؛ إلا أنها غير كافية لكف يد العنف والإجرام الالكتروني ضد المرأة العربية على وجه العموم والجزائرية على وجه الخصوص.

Summary:

Despite the technological development, women continue to suffering from violence and cyber-crime. Image of women still exposure on the web pages with most egregious ways and pornography, by using Spyware on her own life, and theft of data and pictures, and sexually harassed by hackers and criminal-mail.

It also vulnerable to various threats and murder attempts on Web pages, these attempts do not stop, but it is increasing. And this is what is threatening the private life of women: marital and professional. Although the legal attempts to fight against cyber-crime; but it are not enough to desist e-crime against Arab women in general and Algeria in particular.



مقدمة:

عالم الجريمة في اتساع مستمر ومقلق، حيث يتقدم بتقدم وتطور البحوث العلمية والوسائل الالكترونية المتطورة باستمرار لا نظير له،" < لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديثة > تقول روي جودسون، ويضيفP-Bouzat منها لازدياد معدل الجريمة <بأن التزايد فيمعدل الحوادث ما هو إلا بسبب دخول الآلة وعلى وجه الخصوص وسائل النقل التي أحدثت الزيادة المطردة و المقلقة للجرائم غير العمدية>"[1] ؛ بهذا يتضح جليا بان الجريمة هي الجريمة، قد تختلف وسائلها لكن مسبباتها وأثارها متشابهة إلى حد بعيد، بالإضافة إلى أن هذه التطورات التكنولوجية في الحقيقة من أهم مسببات تزايد عدد الجرائم، ربما لتوفرها، وربما لسرعة تنفيذها، وربما لقدرة التنكر ولاختفاء ورائها عند ارتكاب الجرائم.

إذ في تعاملاتنا البنكية، والمدنية، المدرسية والتجارية وحتى السياسية، لا يمكن إغفال جهاز الحاسوب أو شبكة الإنترنت ولا حتى الهاتف النقال. حيث أصبحت وسائل لا مجال للاستغناء عنها، ورغم أن هذه الوسائل التكنولوجية الحديثة قدمت الكثير من الخدمات التي تهدف إلى تسهيل حياة الأفراد وتعاملاتهم ومعيشتهم وحتى حمايتهم من السرقات والاعتداءات...إلا أنها أصبحت عنصرا فعالا في التخطيط وتنفيذ الجرائم ، هذه الأخيرة التي ترتكز على ما توفره الشبكة العنكبوتية من معلومات وبيانات وما القرصنة إلى الوجه الصريح لمثل هذه الجرائم،إذ بات من السهل سرقة مبالغ طائلة بسهولة كبيرة وأنت جالس وراء جهاز كومبيوتر.

حيث يمكن للسارق الالكتروني الحصول على المعلومات الالكترونية ونقلها وتخزينها على الشبكات بطرق تكنولوجية حديثة ومتطورة يصعب في كثير من الأحيان التصدي لها أو إيقاف مسارها. وقد مست هذه الجرائم جميع المجالات وكل الشرائح حتى المرأة لم تسلم منها، حيث تمارس ضدها كل أنواع الجرائم من تحرشات جنسية وسرقات للمعلومات الخاصة والمهنية وسرقة صورها بغرض ابتزازها، كما أن بيع النساء وإقحامها في المنظمات المشبوهة والعصابات الخاصة بالدعارة والتجارة المخدرات وتستخدم حتى كطعم لجلب ضحايا آخرين من الجنسين. هذه الجرائم لا تتعلق فقط بالفتاة القاصر بل تعاني منها كل النساء القاصرات والراشدات، العاملات والماكثات في البيوت، المتعلمات وغير المتعلمات، الغربيات والشرقيات العربيات والجزائريات. فاتساع شبكة الانترنت وعدم محدوديتها الجغرافية جعلت من الجريمة الالكترونية هي الأخرى عابرة للقارات والفئات العمرية.

الانترنت ورغم مميزاتها إلا أن سلبيتها هي الأخرى كثيرة ولا تحصى منها: " الافتقار إلى السرية، واحتوائها على معلومات غير أخلاقية وتافهة، أي انتشار ما يسمى بالإباحية الالكترونية مثل تبادل الصور المؤذية للأخلاقي والقيم، الترويج لمعلومات متطرفة دينيا وسياسيا وعنصريا. بالإضافة إلى انتشار الجريمة الالكترونية منها: جرائم الملكية الفكرية، سرقة البرامج، والاحتيال المالي من خلال بطاقات الائتمان..."[2] ومن خلال ما تم عرضه تطرح هذه الورقة تساؤلات مهمة منها:

- ✓ هل الجانب القانوني كاف لمحاربة ظاهرة الجريمة الالكترونية؟
- ✓ وما هي أهم الجرائم الالكترونية التي تمارس ضد المرأة على صفحات الانترنت؟
- ✓ ما هي طرق الوقاية التي تحمي المرأة من الوقوع كضحية للجرائم الالكترونية؟

---

[1] باطلي، غنية. (٢٠١٥). الجريمة الالكترونية: دراسة مقارنة. الجزائر: الدار الجزائرية. ص ٧-٦

[2] الدليمي، عبد الرزاق. (٢٠١١). الإعلام الجديد والصحافة الإلكترونية. (ط.١). عمان: دار وائل للنشر والتوزيع. ص٦١-٦٢



منهجية للدراسة:

- ✓ **أهمية الدراسة**: تتمثل أهمية الدراسة في النقاط التالية:
  - ✓ التطور التكنولوجي الهائل وما صاحبه من تطورات على مستوى جميع المجالات حتى على مستوى الجريمة.
  - ✓ زيادة انتشار نسبة الجرائم الالكترونية بشكل واسع وملفت للنظر، حيث يتلقى المجرم السيبيري دورات تكوينية في البرمجيات الخبيثة وغيرها...
  - ✓ خطورة ظاهرة الإجرام الالكتروني بسبب مزاياه من سرعة على التنفيذ والقدرة على التخفي والتنوع في الجرائم.
  - ✓ أهمية نصف المجتمع والمتمثل في المرأة، التي تعتبر مسئولة على النصف الثاني من المجتمع.
  - ✓ المساس بسمعة المرأة وتشويه صورتها لا يضرها فقط بل يضر بكل عائلتها وأبنائها والمجتمع على العموم.
  - ✓ الجانب القانوني لا يكفي لوحده لمحاربة الجريمة الالكترونية ضد المرأة.
  - ✓ ضرورة توعية المرأة والمجتمع بالآثار السلبية والخطيرة لهذا النوع من الجرائم وتهديدها لحياة المرأة وتماسك المجتمع.
- ✓ **أهداف الدراسة**: تتمثل أهداف الدراسة في:
  - ✓ الإطلاع على ما كتب حول الجريمة الالكترونية بصورة عامة.
  - ✓ تحديد نوع الجرائم الالكترونية التي تمارس ضد المرأة على صفحات الانترنت.
  - ✓ عرض بعض الحالات التي كانت فيها المرأة والفتاة ضحية الجريمة الإلكترونية.
  - ✓ اقتراح طرق وقائية تحمي المرأة وتساعدها على التصدي لهذا النوع من الجرائم والتهديدات.
  - ✓ تبيان خطورة الجريمة الالكترونية وضرورة التصدي لها.
- ✓ **حدود الدراسة**:

اتبعت الدراسة الاستطلاعية الحالية طريقة عرض بعض الحالات من النساء والفتيات اللاتي تعرضن لجرائم الكترونية متنوعة على صفحات الانترنت وخاصة على صفحات التواصل الاجتماعي وعلى رأسها الفيسبوك. مع الحرص على عدم ذكر التفاصيل كحق لأفراد العينة اللواتي طالبن بذلك. كما حاولت الدراسة طرح عدة نقاط وقائية لحماية المرأة من هذه الجرائم. وهذا من خلال مجموعة من المقابلات غير الموجهة الغرض منها معرفة الجريمة التي تعرضن لها، مع عرض حالة من صفحات الانترنت كنموذج.

الإطار النظري للدراسة:

أولا: تعريف الجريمة الالكترونية:

" تتكون الجريمة الإلكترونية (cyber crimes)أو الافتراضية من مقطعين هما الجريمة(crime) والإلكترونية (cyber). ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات .أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون .والجرائم الإلكترونية هي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت، غرف الدردشة، والبريد الإلكتروني، ويمثل جوهر الجريمة الإلكترونية والموبايل. أبعد من هذا الوصف، ومع ذلك،

فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح"الجريمة الإلكترونية."" [1]

"وهي نشاط اجرامي تستخدم فيه التقنية الالكترونية (الحاسوب الآلي الرقمي وشبكة الإنترنت) بطريقة (مباشرة أو غير مباشرة) كوسيلة لتنفيذ الفعل الإجرامي المستهدف"[2]. وهنا لابد من الإشارة إلى اختلاف التسميات لهذا النوع من الجرائم مثل جرائم الكومبيوتر وجرائم الانترنت أو جرائم التكنولوجيا و الجريمة الافتراضية. أو الانحراف الافتراضي و الجريمة السيبيرية cyber crime أو جرائم التقنية العالية hi-tech crime

كما" أنه لا بد أن نشير بغياب مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فالبعض يطلق عليها جريمة الغش ألمعلوماتي والبعض الأخر يطلق عليها جريمة الاختلاس ألمعلوماتي أو الاحتيال ألمعلماتي وآخرون يفضلون تسميتها بالجريمة المعلوماتية. "[3] وهذا دليل أخر على صعوبة التعامل مع مثل هذا النوع من الجرائم. كما تزداد الصعوبة إذا علمنا بان المشرعون يختلفون في تسميتها جريمة الكترونية إذا لا يعتبرونها جريمة إذا كانت تعتمد على الوسائل الالكترونية فقط، إذ لا بد أن يكون موضوعها أيضا الكترونيا كسرقة حساب الكتروني.

بهذا الصدد "يجب أن نفرق بين ثلاث أنواع مختلفة من جرائم الكومبيوتر: الجرائم التي يستخدم فيها الكومبيوتر كأداة مثل الاحتيال، والجرائم التي يكون الكومبيوتر فيها محل الجريمة، مثل اختراق أجهزة الكومبيوتر وإرسال الفيروسات، والجرائم التي يكون دور الكومبيوتر فيها ثانوي فيما يتعلق بالجريمة، ومثال ذلك عند استخدامه كوسيط لتخزين سجلات العمليات الإجرامية. "[4]

و لتباين خطورة هذه الظاهرة تعرض بعض الإحصائيات " في بريطانيا عام٢٠٠ هناك جريمة الكترونية تقع كل١٠ ثواني (٣ مليون جريمة بالسنة) وأكبر نسبة فيها تعود لجرائم التحرش الجنسي٨٥٠ ألف حالة) بينما هناك٩٢ ألف حالة لسرقة الهوية،و١٤٥ ألف حالة لاختراق الحواسيب بهدف سرقة المعلومات أو التخريب٢٠٧ ألف حالة للحصول على الأموال من خلال الاحتيال للسطو على أرقام البطاقات الائتمانية. "[5] " كما أن هناك حوالي٨٠ % من أعمال الجريمة الالكترونية تنشأ في شكل من أشكال النشاط المنظم، مع سوق الجرائم الالكترونية الأسود، على شكل عمل دورة البرمجيات الخبيثة، وفيروسات الكومبيوتر...وبيع البيانات وقبض ثمن المعلومات المالية. "[6]

ثانيا: تصنيف الجرائم المعلوماتية الواقعة على الأشخاص:

١ - **جرائم القذف والسب وتشويه السمعة:** "تعد جرائم السب والقذف الأكثر شيوعا في نطاق الشبكة، حيث يستعمل الجاني حسب القواعد العامة جرائم القذف والسب عبارات بذيئة تمس وتخدش شرف المجني عليه، بل إن إرادته

---

[1] البداينة، ذياب. (٢-٤ سبتمبر ٢٠١٤). الجرائم الالكترونية: المفهوم والأسباب. ورقة عمل مقدمة ضمن فعاليات الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الأردن. ص٤

[2] عبد الله، عبد الله. (٢٠٠٧). جرائم المعلوماتية والإنترنت:(الجرائم الالكترونية)،(ط.١). بيروت: منشورات الحلبي الحقوقية. ص15

[3] عكور، سومية. (٢-٤ سبتمبر ٢٠١٤). الجرائم المعلوماتية وطرق مواجهتها: قراءة في المشهد القانوني والأمني. ورقة عمل مقدمة ضمن فعاليات الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الأردن. ص ٣

[4] السنباطي، ايهاب. (جويلية، ٢٠٠٧). الجرائم الالكترونية : (الجرائم السيبيرية): قضيية جديدة آم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد. أعمال الندوة الإقليمية حول : الجرائم المتصلة بالكومبيوتر. المملكة المغربية.ص٢٠

[5] مصطفى سمير و سلمان محمود وعبد الرحمن حسن. (د.ت). الجريمة الالكترونية عبر الانترنت أثرها وسبل مواجهاتها. ص ٤

[6] البداينة، ذياب. المرجع السابق، ص ٩

اتجهت لذلك بالذات. وبالتطور أصبحت الانترنت إحدى هذه الوسائل إن لم نقل أكثرها رواجا-فعادة ترسل عبارات السب والقذف عبر البريد الصوتي أو ترسم أو تكتب على صفحات الويب ما يؤدي بكل من يدخل هذا الموقع لمشاهدتها أو الاستماع إليها، ويتحقق بذلك ركن العلنية الذي تطلبه الكثير من التشريعات في السب العلني، وإذا لم يطلع عليها أحد فإنه يمكن تطبيق مواد السب أو القذف غير العلني."[1]

٢ - صناعة ونشر الإباحة:

" كما وضحت دراسة أدست (Adsit, 1999) أن المواقع الإباحية أصبحت مشكلة حقيقية وأن الآثار المدمرة لهذه المواقع لا تقتصر على مجتمع دون الآخر، ويمكن أن يلمس أثارها السيئة على ارتفاع جرائم الاغتصاب بصفة عامة واغتصاب الأطفال بصفة خاصة، العنف الجنسي، فقد العائلة لقيمها ومبادئها وتغيير الشعور نحو النساء إلى الابتذال بدل الاحترام. ويبدوا أن لكثرة المواقع الإباحية على الإنترنت والتي يقدر عددها بحوالي (٧) ألف موقع دور كبير في إدمان مستخدمي الإنترنت عليها حيث أتضح أن نسبة (١٥ ٪) من مستخدمي الإنترنت البالغ عددهم (٩٠) مليون شخص تصفحوا المواقع الإباحية في شهر ابريل عام (١٩٩٩)"[2]

٣ - جريمة التهديد والمضايقة

"يقصد بالتهديد الوعيد بالشر، وهو زرع الخوف في النفس بالضغط على إرادة الإنسان،وتخويفه من أضرار ما سيلحقه أو سيلحق أشياء أو أشخاص له بها صلة."[3]

٤ - انتحال الشخصية :وتشمل ما يلي:

أ - جرائم انتحال شخصية الآخرين:

"تعتبر جرائم انتحال شخصية الآخرين من الجرائم القديمة إلا أن التنامي المتزايد لشبكة الإنترنت أعطى قدرة اكبر على جمع المعلومات الشخصية المطلوبة عن الضحية والاستفادة منها في ارتكاب جرائمهم .فتنتشر في شبكة الإنترنت الكثير من الإعلانات المشبوهة والتي تداعب عادة غريزة الطمع الإنساني في محاولة الاستيلاء على معلومات اختيارية من الضحية، فهناك مثلا إعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية والذي يتطلب بطبيعة الحال الإفصاح عن بعض المعلومات الشخصية كالاسم والعنوان والأهم رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية، وبالرغم من أن مثل هذا الإعلان من الوضوح بمكان انه عملية نصب واحتيال إلا انه ليس من المستبعد أن يقع ضحيته الكثير من مستخدمي الإنترنت .ويمكن أن تؤدي جريمة انتحال الشخصية إلى الاستيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو حتى الإساءة إلى سمعة الضحية .

ب - انتحال شخصية المواقع:

مع أن هذا الأسلوب يعتبر حديث نسبياً، إلا انه اشد خطورة وأكثر صعوبة في اكتشافه من انتحال شخصية الإفراد، حيث يمكن تنفيذ هذا الأسلوب حتى مع المواقع التي يتم الاتصال من خلال نظم الاتصال الأمن حيث يمكن وبسهولة اختراق مثل هذا الحاجز الأمني، وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع

[1] الكعبي، محمد. (د.ت). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت. القاهرة: دار النهضة العربية. ص ٨٨

[2] منشاوي، محمد . جرائم الانترنت من منظور شرعي وقانوني.مكة ١-١١-١٤٢٣ تم الاسترجاع يوم ١٥-١٠-٢٠١٦ من:
http://www.ba-menoufia.com/books-pdf/1304065160509f5b748.pdf

[3] الكعبي، محمد. المرجع السابق. ص ٨٨

بني آو يحاول اختراق موقع لأحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور .ويتوقع أن يكثر استخدام أسلوب انتحال شخصية المواقع في المستقبل نظرا لصعوبة اكتشافها."[1]

ثالثا: أركان الجريمة المعلوماتية

تنهض الجريمة على ركنين رئيسيين هما الركن المادي والركن المعنوي، فلا بد للجريمة المعلوماتية إذن من ركن مادي يمثل كيانها الملموس ويعبر عن إرادة الفاعل بصورة يمكن إثباتها، ولا بد أيضا من ركن معنوي يعبر عن إرادة المجرم ألمعلوماتي.

١ - الركن المادي

لا بد من فعل أو امتناع يمكن إثباته إذ لا عبرة بما يدور في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم ، والركن المادي هنا يختلف من حال لأخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد ، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة

المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تمامًا لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكومبيوتر .وهذا لا يسبب إشكالا، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقتها (التقليدية) ، وهذا ما يدعو للتدخل التشريعي.

٢ - الركن المعنوي

الجريمة ليست كيانا ماديًا خالصًا قوامه الفعل وما يترتب عليه ، بل هي فوق ذلك كيان نفسي ، ذلك أن ماديات الجريمة لا تنشئ لمفردها مسؤولية ، وهذا المنطق يسري على الجرائم المعلوماتية شأنها شأن أية جريمة أخرى ، فلا بد أن ترتكب من شخص قادر على تحمل تبعة أفعاله (مسئول جزائيا) وبذلك لا يسأل عنها من لا يعترف لهم قانون العقوبات بهذه الصفة وهم من كان فاقد الإدراك أو الإرادة .والركن المعنوي بصفة عامة علاقة تربط بين ماديات الجريمة وشخصية الجاني وهذه العلاقة تكون محل لوم للقانون وتتمثل في سيطرة الجاني على سلوكه ونتائج هذا السلوك ، وجوهر هذه العلاقة الإرادة ومن ثم فهي ذات طبيعة نفسية. ومعلوم أن هناك تقسيم للجرائم يعتمد الركن المعنوي أساسا له، وبموجبه تكون الجرائم إما عمديه وإما غير عمديه .[2]

رابعا: أنواع جرائم الحاسب الآلي والإنترنت:

المجموعة الأولي : تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي لاستغلالها بطريقة غير مشروعة كمن يدخل إلى إحدى الشبكات ويحصل على أرقام بطاقات ائتمان يحصل بواسطتها على مبالغ من حساب مالك البطاقة ، وما يميز هذا النوع من الجرائم انه من الصعوبة بمكان اكتشافه ما لم يكن هناك تشابه في بعض أسماء أصحاب هذه البطاقات .

المجموعة الثانية : تستهدف مراكز معالجة البيانات المخزنة في الحاسب الآلي بقصد التلاعب أو تدميرها كليا أو جزئيا ويمثل هذا النوع الفيروسات المرسلة عبر البريد الإلكتروني أو وبواسطة برنامج مسجل في احد الوسائط المتنوعة والخاصة

---

[١] منشاوي محمد. المرجع السابق

[٢] غايب، نصار. الجريمة المعلوماتية. تم الاسترجاع في ١٧-١١-٢٠١٦ من http://www.iasj.net/iasj?func=fulltext&aId=28397

بتسجيل برامج الحاسب الآلي ويمكن اكتشاف مثل هذه الفيروسات في معظم الحالات بواسطة برامج حماية مخصصة للبحث عن هذه الفيروسات ولكن يشترط الأمر تحديث قاعدة بيانات برامج الحماية لضمان أقصى درجة من الحماية.

المجموعة الثالثة: تشمل استخدام الحاسب الآلي لارتكاب جريمة ما، وقد وقعت جريمة من هذا النوع في إحدى الشركات الأمريكية التي تعمل سحبا على جوائز اليانصيب حيث قام احد الموظفين بالشركة بتوجيه الحاسب الآلي لتحديد رقم معين كان قد اختاره هو فذهبت الجائزة إلى شخص بطريقة غير مشروعة.

المجموعة الرابعة: تشمل إساءة استخدام الحاسب الآلي أو استخدامه بشكل غير قانوني من قبل الأشخاص المرخص لهم باستخدامه ومن هذا استخدام الموظف لجهازه بعد انتهاء عمله في أمور لا تخص العمل[1].

خامسا: **خصائص الجريمة المعلوماتية:**

" الجريمة المعلوماتية تتميز بخصائص وصفات تميزها عن غيرها من أنواع الجرائم الأخرى فأول ما يلفت النظر في الجريمة المعلوماتية هو نعومتها وبعدها عن العنف فلا تتطلب لارتكابها العنف ولا استعمال الأدوات الخطرة كالأسلحة وغيرها، فنقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلا لا تحتاج إلا إلى لمسات أزرار .

ثم إن الجريمة المعلوماتية تمتاز أيضا بإمكانية تنفيذها بسرعة فأغلب الجرائم المعلوماتية ترتكب بوقت قصير جداً قد لا يتجاوز الثانية الواحدة، وتتميز الجريمة المعلوماتية أيضاً بإمكانية ارتكابها عن بعد فلا تتطلب وجود فاعل الجريمة في مكان الجريمة؛ بل يمكن للفاعل تنفيذ جريمته في مكان بعيد عن المكان التي يكون فيه، فالشخص القائم على الحاسوب في أحد المصارف في طوكيو يستطيع أن يحول مبلغاً من المال من فرع المصرف في طوكيو. إلى فرعه في برلين في ألمانيا أو نيويورك في الولايات المتحدة الأميركية، وان الغالبية العظمى من الجرائم المعلوماتية التي ترتكب عبر الإنترنت يكون الفاعل في دولة والمجني عنه في دولة أخرى .وهذا أدى إلى ظهور مشاكل تتعلق بالاختصاص المكاني، وجعل التعاون الدولي أمراً محتماً لمواجهة هذا النوع الجديد من الإجرام ومكافحته."[2] نظرا لصعوبة إثبات أركانها وإمكانية التخفي وسرعة الاختفاء بعد ارتكابها.

سادسا: **صفات المجرم ألمعلوماتي:**

لقد تنوعت الدراسات التي تحدد المجرم، وشخصيته ومدى جسامة جرمه كأساس لتبرير وتقدير العقوبة .ويكمن السؤال في حالتنا تلك :كيف يمكن تبرير وتقدير العقوبة في حالة مجرم الكمبيوتر والانترنت وهل هناك نموذج محدد للمجرم ألمعلوماتي؟ بالتأكيد لا يمكن أن يكون هناك نموذج محدد للمجرم ألمعلوماتي، وإنما هناك سمات مشتركة بين هؤلاء المجرمين ويمكن إجمال تلك السمات فيما يلي:

1-**مجرم متخصص** :له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهاراته في اختراق الشبكات وكسر كلمات المرور أو الشفرات، ويسبح في عالم الشبكات ليحصل على كل غالٍ وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسب ومن خلال الشبكات.

2-**مجرم يعود للإجرام** :يتميز المجرم ألمعلوماتي بأنه يعود للجريمة دائمًا، فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات .فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته ومهارته في الاختراق.

---

[1] منشاوي محمد . المرجع السابق.

[2] السالك، كامل. (٢٠٠٠). الجريمة المعلوماتية. ورقة عمل قدمت في مؤتمر للجمعية السورية للمعلوماتية . حلب

3-**مجرم محترف** :له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال.

4-**مجرم ذكي** :حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية، حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب"[1].

الإطار القانوني والوقائي للجريمة الالكترونية ضد المرأة

أولا: **طرق التصدي للجريمة الإلكترونية ضد المرأة**

إن تزايد الجرائم الإلكترونية ضد المرأة بصورة عامة و العربية والجزائرية بصورة خاصة دفع رجال القانون وأصحاب القرار في الدول في التفكير في حلول ناجعة لمحاربة هذا النوع من الجرائم منها القانون الذي يجرم مرتكب السلوك المخالف للقانون المعمول به على شبكات الانترنت أو الوسائل التكنولوجية المتاحة والمختلفة إذ يمكن الرجوع للتسجيلات واقتفاء أثر المجرم بنفس الطريقة الالكترونية وهذا ما يسمى بالشرطة الالكترونية. إذ لا بد من هذا النوع من القانون حتى تكتمل فصول محاكمته كما اكتملت فصول جريمته.

وتظهر أهمية التصدي لمثل هذه الجرائم من خلال اتخاذ التدابير على مستوى الفرد كتعطيل الكاميرات وتغيير كلمة السر كل فترة معينة، وعدم نشر الصور والمعلومات الخاصة خاصة على المواقع التي يدخلها أفراد كثر... وهذا الاهتمام أيضا يظهر على مستوى الدول " والحكومات و المنظمات الدولية من بينها المجلس الأوربي واقتناعا منه بضرورة الحاجة إلى سياسة جنائية مشتركة تهدف إلى حماية المجتمع من الجريمة الالكترونية، وذلك من خلال إقرار التشريع الملائم ودعم التعاون الدولي وإدراكا لعمق التغيرات التي أحدثتها عمليات واستمرار عولمة شبكات الكومبيوتر واهتماما بمخاطر إمكانية استخدام الكومبيوتر والمعلومات الالكترونية في ارتكاب الجرائم، وأن الأدلة المتعلقة بمثل هذه الجرائم يمكن تخزينها ونقلها عبر هذه الشبكة"[2]

نظرا لطبيعة التعامل مع المعطيات على صفحات الانترنت وصعوبة تحديد نوايا المجرم على ذلك فقد اتفق كل من المشرع الفرنسي و الجزائري على " رفع سقف التجريم إلى الأعمال التحضيرية بدل من تجريد العزم المجرد. ولقد نص المشرع الجزائري على العقاب على الاتفاق الجنائي بنص المادة ٣٩٤ مكرر٥ من القانون٠٤-١٥ < يعاقب كل من شارك في مجموعة أو في اتفاق بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة ذاتها. > ويقابل هذا النص المادة٣٢٣-٤ من القانون الجنائي الفرنسي"[3]

إن هذه المادة توفر حماية إضافية لضحايا الجرائم الالكترونية خاصة النساء منهم، إذ لا يكفي لمواجهة خطورة هذا النوع من الجرائم الانتظار حتى الشروع في الجريمة لما تتميز به من سرعة تنفيذ ونقل أكبر قدر ممكن من المعلومات الالكترونية فحينها ستكون الجريمة كاملة الأركان وبالتالي سبل الحماية المتبعة تكون غير كافية لان طبيعة الجريمة الالكترونية ورغم أنها تتضمن نفس الأفعال المادية إلا أنها تختلف في الأدوات المستخدمة بالإضافة إلى سرعة انتشارها كالجرائم التي تمس بسمعة المرأة ونشر صورها بأبشع الطرق. فالوقاية خير من العلاج لردع السلوكيات غير المشروعة في حق الأفراد بصورة عامة والمرأة بصورة خاصة كونها نصف المجتمع وتعبر المسئولة عن النصف الثاني. وتتعدد العقوبات

[1] قطب، محمد. الجرائم المعلوماتية وطرق مواجهتها تم الاسترجاع في ١٠-٢-٢٠١٧ من:/http://www.policemc.gov.bh/mcms-store/pdf

[2] باطلي، غنية. المرجع السابق. ص٨

[3] باطلي، غنية. المرجع نفسه. ص١٩٧

المسلطة على المجرم في حالة الجريمة الكاملة أو التحضير للجريمة بين غرامة مالية والحبس بين شهرين إلى٣ سنوات حسب المشرع الفرنسي. ويمكن عرض دور القانون من خلال النقاط التالية:

" المساعدة القانونية المتبادلة وجرائم الانترنت:

- ✓ ثمة حاجة واضحة لالتزام جميع الدول.
- ✓ ثمة حاجة إلى أن يكون خطاب الطلب مفصلا بقدر الإمكان.
- ✓ لا تقدم طلبا رسميا إلا إذا كنت مضطرا لذلك.
- ✓ إذا قدمت طلبا رسميا ولم تعد بحاجة للمعلومات التي قدمت الطلب من أجلها، ابلغ الدولة الأخرى بذلك.
- ✓ لا تقدم إلا الحد الأدنى من الطلبات وحدد ما تريده على وجه الدقة.

ولكي تقدم طلبا رسميا للحصول على المساعدة، كثيرا ما تجد نفسك مضطرا لأن تدرج في الخطاب معلومات حساسة، وهناك مجموعة من الخطوات لحماية هذه المعلومات الحساسة."[1]

إن القانون وح ده لا يكفي لمحاربة الجريمة الالكترونية لأنه يبقى يعاني من التلاعب القانوني والاصطلاحي وصعوبة تحديد الفاعل بدقة لقدرته على التخفي وعدم سهولة إثبات النوايا بسهولة. كما أن القانون تواجهه مشكلة من نوع آخر وهي إمكانية حدوث تطورات و تغيرات على مستوى الوسائل الالكترونية وطرق التعامل معها مما لا يتماشى مستقبلا مع القوانين التي سنت بخصوصها في فترة سابقة؟ لهذا وجب القيام بعدة خطوات وقائية تجنب المرأة للتعرض لمثل هذه الجرائم ومنها ما يتعلق بالأمور التقنية ومنها ما يتعلق بسلوكيات وأخلاقيات المرأة:

- ✓ استخدام الانترنت في الأمور المفيدة العلمية و المهنية...وليس في الأمور التافهة.
- ✓ إجراء دورات تدريبية حول استخدام الكومبيوتر بطريقة أمنة.
- ✓ توعية المرأة بخطورة الجريمة الالكترونية على جميع مجالات حياتها.
- ✓ توعية المجتمع ببشاعة الاعتداءات الالكترونية على المرأة فه كالاعتداء على كل المجتمع.
- ✓ تبني مستوى أمني وعالي المستوى من طرف الأشخاص والشركات.
- ✓ القيام بمسح دوري على جهاز الكومبيوتر.
- ✓ عدم استخدام الأسماء والصور والمعلومات الخاصة على صفحات الويب إلا للضرورة المهنية والعلمية.
- ✓ تغيير كلمة السر أو المرور Pass Word من حين على أخر و إنشاء جدران الحماية Firewalls.
- ✓ التشفير والتخزين الاحتياطي للمعلومات.
- ✓ التواصل مع الأشخاص الموثقين والمواقع الآمنة قدر الإمكان.
- ✓ عدم إبقاء الجهاز في حالة عمل بشكل مستمر .
- ✓ عدم تشغيل الكاميرات إلا عند الحاجة.
- ✓ عدم الانسياق وراء الإعلانات المغرية والتي تنشرها مؤسسات وأفراد مجهولين المصدر.
- ✓ عدم دخول المواقع المشبوهة لأنها الواجهة التي يستخدمها المجرمون والقراصنة...
- ✓ استخدام البرامج المضادة للفيروسات وتحيينها.
- ✓ عدم تقديم الطلبات الخاصة بطلب المساعدة إلا عن طريق خطوط وأرقام أمنة.

[1] تاينر، السيد. (٢٠٠٧). أهمية التعاون الدولي في منع جرائم الانترنت. أعمال الندوة الإقليمية حول : الجرائم المتصلة بالكومبيوتر . المملكة المغربية.ص١١٥

ثانيا: **الجرائم الالكترونية التي تتعرض لها المرأة**

تتعرض المرأة لعدد غير منته من الجرائم الالكترونية، سواء كانت من مستخدمي الانترنت والوسائل التكنولوجية أم لا، من أمثلتها: " استغلال خدمات الانترنت بإرسال رسائل تحرش ومضايقة أو تشويه وتحقير شخص من خلال البريد الالكتروني فضلا عن إمكانية اختراق البريد الالكتروني والاطلاع على معلوماته. انتشار الفيروسات والديدان وهذا يعني إصابة المعلومات المختزنة بالتلف – أو القرصنة – بالإضافة إلى تجاوز حقوق النشر - والتأليف- المشاكل والمعاكسات الأخلاقية: تتضمن شبكة الانترنت عدد هائل من الصور أو الروايات الجنسية الخليعة، كما أن هناك معلومات تعطى لبعض المستخدمين عن عناوين بيوت الدعارة في العديد من دول العالم. "[1] وغيرها من الجرائم المنافية للأخلاق والمخلة بالحشمة. مثل الجرائم التي يكون البلوتوث Bluetooth وسيلة لها من خلال تبادل الأشرطة العنيفة و ذات المضمون غير الأخلاقي كما يمكن من خلال البلوتوث الاطلاع و التجسس وسرقة الملفات والمعلومات من أجهزة مستخدميه و التجسس على مكالمتهم وتسجيلها، حيث يمكن إجراء اتصال من جهاز الضحية من طرف المجرم الالكتروني يهدد من خلاله الآخرين مثلا. أو الفيس بوك face book مسرحا لها من خلال الصدقات التي لا تكون حقيقية في الغالب و لا يبدو أن نواياها حسنة.

كما تتعرض العديد من النساء إلى سرقة بطاقة الائتمان عن طريق التحايل أو وعود العمل و الزواج الزائفة أو حتى عن طريق جذبهن للمشاركة في عصابات المخدرات والدعارة والإرهاب من خلال برامج جمع المعلومات bots . وما أكثر جرائم الابتزاز والتهديد التي تتعرض لهن النساء خاصة في العلام العربي مقابل نشر معلومات خاصة عنهن أو فبركة صور مخلة بالحياء لهن وتهديديهن بنشرها، بالإضافة إلى جرائم تشويه السمعة للأحياء والأموات منهن فكم من فتاة تم تشويه صورتها الاجتماعية بعد نجاحها أو موتها منتحرة مثلا أو في حادث معين.

ثالثا: **عرض لبعض الحالات الواقعية كانت فيها المرأة الجزائرية ضحية للجريمة الالكترونية**:

إن الانترنت بدل أن تكون وسيلة لمعالجة المشكلات التي تعاني منها المرأة خاصة العنف والجريمة أصبحت مصدرا من مصادر ممارسة العنف والجريمة ضدها. وه ذا من خلال نشر الصور الإباحية وغير الأخلاقية للنساء pornographic images. كما يبدو أن هذا التقدم التكنولوجي امتزج مع العنصرية...لتصعيد الاستغلال الجنسي للنساء وهذا في إطار ما يعرف بصناعة الجنس على الانترنت. فيمكن للرجل ومن خلال صفحات الانترنت الوصول إلى العروض الجنسية الحية، والمواد الإباحية التفاعلية، وطرق شراء المومس، وعبيد الجنس...

وتعتبر صناعة الجنس التي يكون موضوعها في الغالب الفتيات و النساء وحتى الأطفال مصدر تمويل مهم للكثير من محركات البحث ، ورغم هذا فإننا لا ننكر دور الانترنت في محاربة هذه الظواهر ومثيلاتها. فما لا يقل عن: ٥٠٠ امرأة وفتاة يتم الاتجار بهن في الولايات المتحدة و يجهل كيف يتم ذلك على وجه الدقة، ومع ذلك فقد نجحت الانترنت في خلق مواقع خاصة لمكافحة هذه المشاكل مثل توفير مساحة للنساء اللواتي تعرضن للجرائم الالكترونية ومتابعتهم من طرف العديد من المختصين لتقديم المساعدة لهم وكذا بغرض تبادل الخبرات وتحذير الأخريات من الوقوع في نفس المشكلة. وهذا ما دفع بالقائمين عليها التأكيد على ضرورة توفير السلامة لمستخدمي هذه المواقع، من خلال التعامل السري، لأن المشكلة تكمن في أن أغلب النساء لا يعرفن كيفية التنقل بأمان عبر وصلات شبكة الانترنت، فبدل البحث عن المعلومات يكن ضحايا لتنوع هائل من الانتهاكات.

---

[1] الدليمي، عبد الرزاق. المرجع السابق. ص٦٢-٦٣-٦٤

ومن بين هذه الجرائم و الانتهاكات نذكر الحالات الواقعية التالية: مع التنبيه إلى عدم التفصيل فيها مخافة التعرف عليهن وهذا ما تخشاه الحالات: وهي كثيرة...

الحالة الأولى: الاستغلال والتحرش الجنسي

فتاة تتعرض للتحرش الجنسي (عن طريق تبادل الألفاظ والصور...) من طرف أخوها عن طريق الفيس بوك باحثة عن زوج المستقبل لتكتشف الأمر فيما بعد وهي تعيش مع أخيها في نفس البيت وقد عان معا من حالة اكتئاب حاد، رغم أن الأخ لم يعرف الحقيقة لحد الساعة.

الحالة الثانية:التجسس وتسجيل المكالمات

زوجة تطلق بعدما قام زوجها بوضع تقنية تجسس، أو بتثبيت برنامج إنصات على هاتفها النقال وسمعها تتحدث عنه بسوء مع أمها وعائلتها.

الحالة الثالثة: التهديد وتشويه السمعة

فتاة في العشرينات ورغم عدم استخدامها للانترنت طلب منها رجل الزواج فلما رفضت هددها بنشر صورها على الانترنت فلم تنصع له، فقام بوضع صورة وجهها على جسد امرأة عارية بتقنية الفتوشوب، وبذلك نجح في تشويه سمعتها إلى حد كبير ولم تتجاوز هذه الفتاة أثار الجريمة إلا بعد فترة وبمساعدة الأسرة.

الحالة الرابعة:السب والشتم

زوجة تتعرض للسب والشتم من طرف امرأة أخرى بعدما كشفت علاقتها بزوجها وكان البريد الالكتروني والفايس بوك هو الأداة. وقد كانت هذه المجرمة تتخفى وراء اسم مزور غير حقيقي.

الحالة الخامسة: تشويه الصورة و السمعة عن طريق نشر الصور على الحائط

حائط الفيس بوك كان مسرح الجريمة، أشخاص مجهولين ومعروفين قاموا بنشر بعض الصور وتعليقات على حائط شخصية معروفة للنيل منها وإفساد مزاجها كنوع من تصفية الحسابات.

الحالة السادسة: مشكلة استخدام أرقام الهواتف في البريد الالكتروني

الكثير من الفتيات تعرضن لمعاكسات على الإميل وعلى هاتفهن الخلوي بسبب قدرة القراصنة والمجرمين على سرقة معلوماتهم الخاصة ومنها الاسم ورقم الهاتف.

الحالة السابعة: الإساءة لسمعتها بعد موتها

طالبة جامعية لم يعرف سبب موتها هل هو انتحار أم قتل عمدي، تنشر معلومات على صفحات الفيس بوك بأنها كانت حاملا بطريقة غير شرعية فانتحرت.

الحالة الثامنة: خطيب مغشوش

تعرفت عليه عن طريق غرف الدردشة والشات، كان مؤدبا غنيا يريد إنشاء أسرة ويتيم بسبب موت والديه في حادث ولا يملك بيتا وجده يكرهه لأنه يكره أباه، وبعد حصوله على كل المعلومات وعنوان البيت وبعد اللقاء الأول تبين أنه فقير



يريد استغلالها كونها امرأة عاملة. وبدأت سلسلة التهديدات وأقر بأنه كان يكذب بعد٧ أشهر من التعارف على الفيسبوك ولا يعطها أي معلومة صحيحة (وقد يكون مصابا بهوس الكذب)، فأصيبت بصدمة نفسية و تخلت عن العمل.

الحالة التاسعة: التلاعب بالمشاعر والاستغلال العاطفي

فئة جامعية٢٢ سنة تتواصل مع شخصيات مشهور، البداية كانت لأخذ النصيحة والحقيقة لملئ الفراغ العاطفي فوقعت ضحية الكلام المنمق والمعسول ممن يكبرونها سنا ويفترض أنهم مصدر موثوق ثم يتبين فيما بعد أنهم مجرد أشخاص يضيعون الوقت على الدردشة وبعدها يقطعون العلاقة معها مخافة كشفهم.

الحالة العاشرة: التحرش الجنسي بعد علاقة في الفيسبوك ثم التهديد بتشويه السمعة

طالبة جامعية تعرف على شرطي في الفايسبوك دون استخدام خيار الإخفاء لمعلوماتها الشخصية وكان يبدو مهذبا في كلامه، وبعد فترة التعارف لمدة تقل عن شهر اتفقا على لقاء، فتحرش بها جنسيا، وكانت صدمة بالنسبة لها، وهددها بأنه سيخبر الجميع بما فعله بها إن حاولت التخلي عن هذه العلاقة. لكنها استطاعت الخروج من المشكلة بسبب مساعدة الأصدقاء.

حالات أخرى نشرت على الانترنت تحذيرا لباقي الفتيات منها:

الحالة ل.س. سرقة المعلومات و الصور والتشهير بها

اضطرت (ل.س) والتي فضلت عدم ذكر اسمها، وتعمل مسئولة النوع الاجتماعي في إحدى المؤسسات الحكومية، لاستخدام صور رمزية عبر حسابها الخاص على الفيس بوك، عوضا عن صورتها الشخصية، لكي لا يستغل أحد صورتها لأغراض مسيئة!" قرار الامتناع عن نشري لصوري يعود لتجربة شخصية مررت بها قبل قرابة العام، إذ كان لي حساب وصور شخصية على أحد مواقع الصداقة العالمية، ولم يكن أحد يتمكن من مشاهدة تلك الصور إلا الأصدقاء الذين أقبل صداقتهم. وفي أحد الأيام فوجئت باتصالات دولية ومحلية كثيرة على جوالي! أخبرني المتصلين خلالها أنهم عرفوا رقمي وإيميلي وشاهدو صوري عبر بروفايلي! حتى أنهم اخبروني أنني (أون لاين."!!)

وأتبعت (ل.س)تقول" رغم ثقتي ويقيني أن لا أحد يفتح جهازي سويا ، أسرعت عائدة لمكتبي لتفحص كمبيوتري وحساباتي على الإنترنت، فوجدت أنها جميعها مسروقة! وحتى صوري الشخصية والخاصة التي لم أشأ نشرها عبر بروفايلي(لكونها دون حجاب) تم نشرها جميعها،! إضافة لقيام منتحل شخصيتي بإضافة صور ومقاطع فيديوهات مخلة بالآداب في بروفايلي لتشويه سمعتي!. لم أعرف كيف أتصرف حيال الآمر فتركته! ولكن، وبعد فترة زمنية، أراني قريب لي يعمل في الأجهزة الأمنية، صورتي على موبايله! وأخبرني بأن أحد زملاؤه (والذي له حساب هو الآخر على موقع الصداقة العالمي)، حمّل صورتي من ذات الموقع على موبايله!! فاستفزني الموضوع وراسلت الموقع، وحين تم التأكد من أن الحساب حسابي أغلق الحساب."

وتعتقد مسئولة النوع الاجتماعي في إحدى المؤسسات الحكومية، أن الشخص الذي اختراق حسابها وإيميلاتها وبالتالي انتحل شخصيتها، و نشر صورها الشخصية التي كانت على جهاز الكمبيوتر الخاص بالعمل في مكتبها، هو ذات الشخص الذي حضر في إحدى المرات لصيانة جهاز الكمبيوتر في العمل، إذ تتوقع انه ولخبرته قام باستغلالها، بحيث تمكن من سحب كلمات المرور وكلمات السر والصور عن الجهاز بسرعة لم تمكنها من ملاحظته، لذا كان قرارها بالإمتناع عن نشر أي صورة شخصية لها وإن بحجاب، منذ تلك الواقعة.

خاتمة:

تم التطرق في هذه الورقة إلى موضوع الجريمة الالكترونية التي تتعرض لها النساء من خلال تبيان مدى شراسة هذا النوع من الجرائم خاصة كون الضحية امرأة -عربية- لما لهذه المجتمعات من تقاليد الكتمان والخوف من الفضيحة والتكتم وفي الغالب تنصاع المرأة لتهديدات المجرم الالكتروني أو كما يسمى المجرم ألمعلوماتي حتى لا يشوه سمعتها فتخسر بيتها وزوجها وعملها وعائلتها ككل. إذ ورغم كل الجهود المبذولة تبقى إمكانية الوقوف على حقيقة الجريمة الالكترونية صعبا نوعا ما لما يتميز به هذا النوع من الجرائم كما ذكرنا سابقا. واغلب بواعث هذا النوع من الإجرام ضد المرأة ينبع من ذهنية متخلفة لدى المجرم رجلا كان أو امرأة؛ ذهنية تنم عن سلوكيات لا أخلاقية والغيرة والحسد وتفضيل معاقبة الأخر على فشله وحظه العاثر في الحياة، إضافة إلى بواعث الطمع في المال والشهرة الخفية، أو لأغراض ومعتقدات شخصية متعددة منها التمييز بين الجنسين.

ورغم المحاولات المستمرة للتصدي لمثل هذه الجرائم تبقى الوقاية خير من ألف مادة قانونية، إذ يبدو القانون عاجزا نوعا ما في التعامل مع هذا النوع الذي لا يتطلب أركان مادية دائما، أضف إلى ذلك الثغرات التي طالما ميزت القوانين وضيق نصوصها الذي يجد المجرم الالكتروني وغير الالكتروني ملاذا للهروب من تحمل تبعات جريمته. كما انه وتبعا لطبيعة الجريمة الالكترونية الدولية وجب أن يكون هناك قانون دوليا للتصدي لمثل هذه الجرائم وهذا أمر غير مستحيل إلا أنه من الصعب الاتفاق على مضامينه وطرق تطبيقه لاختلاف المنطلقات القانونية لكل دولة أو إقليم.

إلا أنه ولتفادي الأضرار الناجمة عن الجريمة الالكترونية الممارسة في حق المرأة وجب تحديد تعريف واضح وصريح لها، ووضع القوانين على أساس هذا التعريف، على المستوى المحلي والدولي. حيث أن محاربة الجريمة المعلوماتية على مستوى الفرد والوطن أي المستوى المحلي غير كاف ولا فعال وإن كان ذلك ففي إطار ضيق؛ كون أنها جريمة سيبيرية دولية عالمية قد تنطلق من مكان جغرافي محدد لكنها تنتشر عبر العالم.

وعليه فإن نتائج هذه الدراسة تتلخص في كون أن القانون وحده لا يكفي، لما يعاني منه من ضعف وثغرات قانونية ناهيك عن تنوع الجرائم والوسائل الإلكترونية المستخدمة في هذا النوع من الجرائم. لكما أن تطبيق القانون على المستوى المحلي فقط دون وجود اتفاقيات فعالة بين الدول لا يكفي لمحاربة مثل هذه الظواهر. وقد لاحظ الباحث أن أغلب المراجع المطلع عليها حاولت الاهتمام بالجانب القانوني و تبيان نقاط الضعف والقوة فيه، وكذا كانت مواضيعها الجرائم المالية والاحتيال والسطو على حسابات البنوك والمؤسسات والأفراد. ربما على اعتبار أنها الأكثر انتشارا كما اشرنا سابقا في الإحصائيات.

كما تشير هذه الدراسة إلى أهمية الوقاية من هذه المشكلات التي ذكرنا بعض النقاط منها مفصلة والتي تؤكد على التوعية وتحذير النساء والفتيات من مخاطر التعامل مع التكنولوجيا مع جهلن بطرق التعامل مع مخاطرها، واستخدامها دون حاجة لأنها في الغالب تكون عرضة للقرصنة والاحتيال. كما انه ليس من الضروري استخدام المعلومات الخاصة دونما حاجة ملحة لذلك، على اعتبار أن النساء والأطفال أكثر استهدافا على الشبكة العنكبوتية. بالإضافة إلى ما سبق فإن المرأة لم تعد فقط مادة إجرامية إباحية أو موضوع للاستغلال العاطفي والتحرش الجنسي والاستغلال المالي، بل أصبحت عنصر فعال في النشر والترويج لظاهرة الإرهاب وتكوين الخلايا المتحركة تحت أغطية متنوعة وكذا في نشر الفكر التطرفي لهذه الخلايا.

قائمة المراجع:

١. **باطلي، غنية**. (٢٠١٥). الجريمة الالكترونية: دراسة مقارنة. الجزائر: الدار الجزائرية
٢. **البداينة، ذياب**. (٢-٤ سبتمبر ٢٠١٤). الجرائم الالكترونية: المفهوم والأسباب. ورقة عمل مقدمة ضمن فعاليات الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الأردن.
٣. **عكور، سومية**. (٢-٤ سبتمبر ٢٠١٤). الجرائم المعلوماتية وطرق مواجهتها: قراءة في المشهد القانوني والأمني. ورقة عمل مقدمة ضمن فعاليات الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الأردن
٤. **الدليمي، عبد الرزاق**. (٢٠١١). الإعلام الجديد والصحافة الإلكترونية. (ط.١). عمان: دار وائل للنشر والتوزيع.
٥. **السنباطي، إيهاب** . (جويليه، ٢٠٠٧). الجرائم الالكترونية : (الجرائم السيبيرية): قضية جديدة ام فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد. أعمال الندوة الإقليمية حول : الجرائم المتصلة بالكومبيوتر. المملكة المغربية.
٦. **عبد الله، عبد الله**. (٢٠٠٧). جرائم المعلوماتية والإنترنت:(الجرائم الالكترونية)،(ط.١). بيروت: منشورات الحلبي الحقوقية.
٧. **تاير، السيد**. (جويلية، ٢٠٠٧). أهمية التعاون الدولي في منع جرائم الانترنت. أعمال الندوة الإقليمية حول : الجرائم المتصلة بالكومبيوتر. المملكة المغربية.
٨. **منشاوي، محمد**. (١-١١-١٤٢٣). جرائم الانترنت من منظور شرعي وقانوني.مكة. تم الاسترجاع يوم ١٥-١٠-٢٠١٦ من : http://www.ba-menoufia.com/books-pdf/1304065160509f5b748.pdf
٩. **السالك، كامل**. (٢٠٠٠). الجريمة المعلوماتية. ورقة عمل قدمت في مؤتمر للجمعية السورية للمعلوماتية . حلب
١٠. **مصطفى سمير وسلمان محمود وعبد الرحمن حسن**.(د.ت).الجريمة الالكترونية عبر الانترنت أثرها وسبل مواجهاتها.ص ٤
١١. **الكعبي، محمد**. (د.ت). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت. القاهرة: دار النهضة العربية.
١٢. **غايب، نصار**. الجريمة المعلوماتية. تم الاسترجاع في ١٧-١١-٢٠١٦ من http://www.iasj.net/iasj?func=fulltext&aId=28397
١٣. **قطب، محمد**. الجرائم المعلوماتية وطرق مواجهتها تم الاسترجاع في ١٠-٢-٢٠١٧ من : http://www.policemc.gov.bh/mcms-store/pdf/



إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية :

(دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام).

الدكتورة أمحمدي بوزينة أمنة أستاذة محاضرة صنف (أ)

كلية الحقوق والعلوم السياسية جامعة حسيبة بن بوعلي-الشلف

مخبر القانون والأمن الإنساني ورئيسة تحرير مجلة جيل حقوق الإنسان

ملخص

بالرغم من ما للثورة المعلوماتية من ايجابياتها وقدرتها على تغيير أوجه الحياة إلى الأحسن والأفضل، إلا أن هذه الثورة المعلوماتية ذاتها تحمل في طياتها أيضا العديد من السلبيات التي تتمثل في الاستخدام غير المشروع لنظم الحاسوب الآلي، ومن هذا المنطلق استطاع الجناة تطوير طرق الإجرام على نحو عال من التقنية في بيئة تكنولوجيا المعلومات.

وفي ظل تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، استدعى الأمر تدخلا تشريعيا صريحا سواء على المستوى الدولي أو الداخلي، فدوليا وضعت أول اتفاقية حول الإجرام المعلوماتي بتاريخ ٠٨/١١/٢٠٠١ تضمنت مختلف أشكال الإجرام المعلوماتي، أما على المستوى الوطني، فقد استدرك المشرع الجزائري الفراغ القانوني من خلال تعديل قانون العقوبات بموجب القانون ٠٤-١٥ باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات"، ويشمل المواد من (٣٩٤ مكرر) إلى (٣٩٤ مكرر ٧)، وكذلك تقررت عقوبات للاعتداء على أنظمة المعلومات في قانون حماية حقوق المؤلف رقم ٠٣-٠٥، كما تقررت عقوبات للاعتداء على أنظمة المعلومات في إطار نفس القانونين، كذلك إضافة إلى الإجراءات المتبعة في التحري في مجال الجرائم المعلوماتية؛ تم استحدث إجراءات تحري خاصة بموجب المادة ٦٥ مكرر ٥ من قانون الإجراءات الجزائية الجزائري وما بعدها؛ كذلك كرس المشرع الجزائري من خلال القانون رقم ٠٩-٠٤ قواعد تحري وحجز وتحقيق خاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

الكلمات الدالة: الحاسوب، النسخ، الاعتداء على أنظمة المعلومات، قواعد التحري الخاصة بجرائم الإعلام والاتصال.

Résumé :

Bien que la révolution des moyens de télécommunications apporte de nobreux points positifs et leur capacité à modifier les aspects de la vie, cette révolution de comporte en elle-même de nombreux inconvénients de l'utilisation illicite de systèmes informatiques automatisés, et constitue un moyen pour la criminalité dans un environnement des technologies de l'information.

Elle encourage les attaques et les systèmes d'information, notamment suite à l'insuffisance de la protection des administrateurs, nécessaire d'intervention législative explicite soit au niveau international ou national, dans un contexte international la première convention élaboré sur la criminalité dans le domaine de l'information, en date du 08/11/2001 contenaient des diverses formes de criminalité à l'information, au niveau national, le législateur algérien a comblé quelque trous juridique grâce à la modification apportée au Code pénal par la loi 04/15 concernant la section VII bis du chapitre III de la deuxième partie du troisième livre intitulé "préjudice des régimes de traitement automatiques des données ", les articles 394 bis) À 394 bis 7) en consacrant de sanctions contre le crime des systèmes d'information dans la loi sur la protection des droits d'auteur, No 03/05, et établi des peines de sévices sur les systèmes d'information dans le cadre de la même loi, ainsi que la procédure d'enquête dans le domaine des délits informatiques; il a été mis au point Procédures d'étudier en particulier en vertu de l'article 65 bis 5 du Code de procédure pénale algérien et au-delà; en outre le législateur algérien, par la loi No 09/04 de bases de détection et la saisie et en particulier de la prévention des délits liés aux technologies de l'information et de la communication et de lutte.

***Mots clés**: Ordinateur, Le plagiat, la violation des systèmes d'information, Les règles spéciales d'investigation contre les crimes de l'information et de la communication.*

Abstract:

It encourages the attacks and the information systems, in particular as a result of the inadequate protection of the administrators, necessary to legislative intervention either explicit at the international or the national level, in an international context The first Convention elaborated on crime in the domain of information, date of 08/11/2001 contained various forms of crime in the information, at the national level, the Algerian legislature has filled some legal holes through the amendment to the Penal Code by the Act 04/15 concerning the Section VII bis of chapter III of the second part of the third book entitled "Injury Treatment regimes of automatic data", articles 394 bis) to 394 bis 7), devoting of sanctions against the crime of systems Information in the Act on the protection of the rights of author, No. 03/05, and established penalties of abuse on information systems in the framework of the same act, as well as the inquiry procedure in the field of computer crimes; it was developed procedures for studying in particular under article 65 bis 5 of the Algerian Code of Criminal Procedure and beyond; in addition the Algerian legislature, by Act No. 09/04 of bases of detection and seizure and in particular the prevention of offenses related to the technologies of the information and of the communication and the fight. Words indicating: computing, of copies, the attack of information systems, special rules of investigation for crimes of the information and of the communication.

***Key words**: computer, plagiarism, the violation of information systems, the special rules of investigation against the crimes of the information and of the communication*

مقدمة

لا شك أن الحاسوب أصبح ضرورة لا يمكن الإستغناء عنها في حياة الأفراد والمؤسسات الخاصة والعامة على حد سواء فقد ساعد على القيام بالأعمال الإدارية والفنية والخدمية التي لا حصر لها، ولكنه في المقابل ساهم بشكل غير مباشر في فتح المجال نحو وجود سلوكيات جديدة وأساليب مختلفة لإرتكاب أفعال غير سوية وجرائم مختلفة، ولاشك أن المجرمين يحاولون الإستفادة من هذا التقدم التقني خاصة وأننا في عصر ثورة المعلومات وتقدم العلوم الحديثة والتكنولوجيا المتطورة، وتبعا لذلك، فإنه من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق، وهذا ليس قاصرا على أسباب التقدم التقني فقط، بل يحدث دوما وبصفة مستمرة، فالمجرم والجريمة في تقدم وتجدد مستمر، فمجرم الأمس ليس كمجرم اليوم، حيث أن هذه التقنيات شجعت وساعدت المجرمين على زيادة عدد وحجم جرائمهم، بل مع انخفاض احتمالات انكشاف أمرهم، مما أدى إلى تزايد حجم الخسائر المادية لجرائم الحاسوب، فبات من الضروري تحديد حجم وأنماط هذه الجرائم، وهو ما سيبرز من خلال الوقوف على جريمة المساس بأنظمة المعالجة الآلية للمعطيات؛ على أن نتعرف قبل ذلك على نظام المعالجة الآلية للمعطيات.

وإن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، استدعى تدخلا تشريعيا صريحا سواء على المستوى الدولي أو الداخلي، فدوليا وضعت أول اتفاقية حول الإجرام المعلوماتي بتاريخ ٠٨/١١/٢٠٠١ تضمنت مختلف أشكال الإجرام المعلوماتي، أما على المستوى الوطني، فقد استدرك المشرع الجزائري الفراغ القانوني من خلال تعديل قانون العقوبات بموجب القانون ٠٤-١٥ باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات"، ويشمل المواد من ٣٩٤ مكرر إلى ٣٩٤ مكرر٧، وكذلك تقررت عقوبات للاعتداء على أنظمة المعلومات في قانون حماية حقوق المؤلف رقم ٠٣-٠٥.

هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات كشرط مسبق بخلاف الاعتداءات على منتجات النظام، وتكشف عن أهم التحديات القانونية التي تفرضها جرائم المساس بأنظمة الكومبيوتر على النظام المعلوماتي الجزائري بشكل خاص والعالمي بشكل عام، ولتحقيق هذا الهدف يحاول هذا البحث بشكل مجمل تقديم صورة عامة لأبرز التحديات المصاحبة لشبكة الإنترنت، من هذا المنطلق، نتساءل ما هي أبرز الأنماط الإجرامية في مجال المساس بأنظمة الكومبيوتر والإنترنت؟، وما هي الجهود المتخذة من قبل المشرع الجزائري في مجال مكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات؟.

إضافة إلى ما سبق، تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإثباتها بسبب ارتكابها بطريقة تقنية كثيرة التعقيد وسهولة تدمير ومحو المعلومات الخاصة بارتكابها وأنها أيضا ذات طبيعة دولية متعدية الحدود حيث تتجاوز الفواصل الجغرافية لعدة دول، فمثلا الدراسة التي قامت بها شركة (Symantec) وهي شركة مختصة في حماية الأنظمة والبرامج المعلوماتية سنة 2010، بينت فيها أن الاعتداءات على الأنظمة المعلوماتية وإصلاحها سنويا يسبب خسارة مالية قدرها 114 مليار دولار في العالم وأن هذه الاعتداءات مست 431 مليون شخص".

ولعل خصوصية الجريمة المعلوماتية، أبرزت مشكلة المكافحة الإجرائية للجريمة المعلوماتية خاصة من ناحية كيفية جمع الأدلة الإلكترونية ومدى حجيتها، وحتى تتوفر في الدليل الإلكتروني المشروعية التي تشترطها القوانين في كافة التشريعات.

والمشرع الجزائري، اقتداء بالمشرعين الذين سبقوه، سارع لمواكبة هذا التطور الذي لحق الجريمة بمكافحتها من الناحية الإجرائية، وذلك بتعديل بعض المواد في قانون الإجراءات الجزائية وإصدار قوانين خاصة وجديدة في مجال الإجراءات.

من هنا تهدف دراستنا التطرق لموضوع آليات الكشف عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، قصد التنبيه إلى واقع تفشي ظاهرة الإجرام المعلوماتي، وعليه، نتساءل عن مدى فعالية السياسة الجنائية المتبعة من قبل المشرع الجزائري في مجال التحري والكشف ومكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات؟.

للإجابة على هذه التساؤلات وحل الإشكال المطروح، نقدم تحليلا يقوم على المحاور التالية:

المبحث الأول: إجراءات التحري الكلاسيكية للكشف عن الجرائم المعلوماتية.

المبحث الثاني: إجراءات التحري المستحدثة للكشف عن الجرائم المعلوماتية.

المبحث الأول

إجراءات التحري الكلاسيكية للكشف عن الجرائم المعلوماتية

في مجال المكافحة الإجرائية للجريمة المعلوماتية، يتعين الإشارة إلى الدور الذي تلعبه الشرطة القضائية كأداة رئيسية لصيانة أمن المجتمع وحمايته من الجرائم بصفة عامة والجرائم المعلوماتية بصفة خاصة، حيث نظرا لطبيعة هذه الأخيرة الخاصة وكيان بيئتها غير المحسوس؛ تظهر صعوبة دور الشرطة في الكشف عنها ومتابعة مرتكبيها، الأمر الذي أدى بالدول السباقة في مكافحة الإجرام المعلوماتي إلى إيجاد وحدات من الشرطة متخصصة بالعمل في هذا المجال، تكون مزودة بالخبراء المدربين وتنظيم دورات لهم للتخصص في مجال مكافحة الجريمة المعلوماتية، وذلك بتلقينهم المعلومات الخاصة بتقنية الحاسوبات والجوانب الفنية لها حتى تسهل عليهم عملية الكشف عن الجرائم ومنع وقوعها بإحكام الرقابة على المحلات العامة كنوادي الأنترنت... الخ، والتي تعد المجال الخصب لاقتراف جرائم المعلوماتية[1]، وكمثال على هذه الوحدات المتخصصة: الوحدة المركزية لمكافحة الجريمة المرتبطة بتكنولوجيا المعلومات والاتصالات المنشأة بموجب مرسوم صادر عن وزارة الداخلية الفرنسية (OCLCTIC) في ماي 2000 والتي تم ضمها لمديرية الشرطة القضائية، مهمتها العمل بالتعاون مع وحدات التحقيق في جرائم الغش في تكنولوجيا المعلومات ، وعليه سوف نبرز هذه الإجراءات فيما يلي:

المطلب الأول: معاينة مسرح جرائم المساس بأنظمة المعالجة الألية للمعطيات

عند التكلم عن المكافحة الإجرائية للجريمة المعلوماتية، أول ما يجب دراسته هو معاينة مسرح الجريمة المعلوماتية: ويقصد بهذه الأخيرة رؤية العين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة [2]، أو هي إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة وهي تتطلب أن ينتقل مأمور الضبط القضائي إلى مكان ما لمباشرتها لإثبات حالته وحالة ما قد يوجد فيه من أشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة محل الإجراء."

---

(1) طارق الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، 2009، ص 422.

(2) محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الجديدة، 2008، ص 123 وما بعدها.

وهي إجراء جائز في كافة الجرائم، إلا أن غالبية التشريعات بما فيها التشريع الجزائري في المادة[61] من قانون الإجراءات الجزائية الجزائري، تقصرها على الجنايات والجنح الهامة، بحيث تعد إجراء وجوبيا في الجنايات وجوازيا في الجنح، وهي قد تتم في مكان عام أو مكان خاص، فإذا كانت في مكان عام؛ فمأمور الضبط القضائي لا يحتاج إلى إذن أو ندب سلطة تحقيق بإجرائها، أما إذا كانت بمكان خاص؛ فلابد لصحتها، إما رضا حائز المكان أو وجود إذن مسبق من سلطة التحقيق بإجرائها.

والهدف من إجراء المعاينة هو ضبط ما استعمل في ارتكاب الجريمة أو نتج عنها، ووضع الأختام في الأماكن التي أجريت فيها المعاينة، إذا وجدت آثار أو أشياء تفيد في الكشف عن الجريمة، كما يجوز لمأمور الضبط القضائي أن يعين حراسا على هذه الأماكن مع ضرورة إخطار النيابة العامة بهذه الإجراءات.

ولمعاينة مسرح الجرائم المعلوماتية، يجب التفرقة بين حالتين:

أ -معاينة الجرائم الواقعة على المكونات المادية للحاسوب (Hardware): كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي المحسوس، فهي لا تثير أية مشكلة بحيث يمكن لمأمور الضبط القضائي معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.

ب -معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها (Software): كتلك الواقعة على برامج الحاسوب وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدته، وهذه الصعوبات، تتلخص فيما يلي:

- قلة الآثار المادية المترتبة عن الجرائم التي تقع على المكونات غير المادية للحاسوب.
- الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة، وذلك بين اقتراف الجريمة والكشف عنها، الأمر الذي يمنح فرصة لإحداث تغييرات أو العبث بالآثار المادية أو زوال بعضها، مما يؤدي إلى غموض الدليل المستقى من المعاينة.

ولنجاح المعاينة في الجرائم المعلوماتية يوصي الخبراء بوجوب إتباع ومراعاة قواعد وإرشادات فنية أبرزها ما يلي:

- القيام بتصوير الحاسوب وما قد يتصل به من أجهزة ظرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة مع التركيز على تصوير أجزائه الخلفية وملحقاته، ومراعاة تسجيل الزمان والتاريخ والمكان الذي التقطت فيه كل صورة.
- يجب ملاحظة واثبات الحالة التي تكون عليها توصيلات الكابلات (الخيوط الكهربائية للحاسوب)، والتي تكون متصلة بمكونات النظام، حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة.
- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو للبيانات المسجلة.
- وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم.
- ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.
- إبعاد الموظفين عن أجهزة الحاسب الآلي وكذلك عن الأماكن التي توجد بها أجهزة أخرى.
- التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة، والأشرطة والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، ورفع البصمات التي قد تكون لها صلة بمرتكبي الجريمة.
- القيام بحفظ المستندات الخاصة بالإدخال، وكذا مخرجات الحاسوب الورقية التي قد تكون ذات صلة بالجريمة، وذلك من أجل رفع ومضاهاة البصمات التي قد تكون موجودة عليها.

- يجب أن تقتصر مباشرة عملية المعاينة على مأموري الضبط وفئة الباحثين، ممن تتوافر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحاسوب واسترجاع المعلومات، وممن تلقوا التدريب الكافي لمواجهة هذه النوعية من الجرائم، والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة، ففي فرنسا مثلا، يقوم فريق مكون من١٣ شرطي بالإشراف على تنفيذ المهمات التي يعهد بها إلى وكلاء النيابة والمحققين، وهم قد تلقوا تدريب متخصص إلى جانب اختصاصهم الأساسي في مجال التكنولوجيا الحديثة، وهم يقومون بمرافقة المحققين أثناء التفتيش، حيث يقومون بفحص كل جهاز وينقلون نسخة من الاسطوانة الصلبة وبيانات البريد الالكتروني ثم يقومون بتحرير تقرير يرسل إلى القاضي الذي يتولى التحقيق[1].

أما عن المعدات والبرامج، فهم يستخدمون برامج تستطيع استعادة المعلومات من على الأسطوانة الصلبة ن كما يمكنها قراءة الاسطوانات المرنة والصلبة التالفة، كما يوجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات المحمولة ومن المهم هنا أن يتم توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد، مع توثيق كل دليل على حدى بما فيها الأدلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها، ومن قام برفعه وتحريزه وكيف ومتى تم ذلك.

المطلب الثاني: إجراءات تفتيش النظم المعلوماتية وضبطها

إن الهدف من التفتيش هو ضبط الأدلة المادية للكشف عن الجريمة، فكل ما يضبطه مأمور الضبط القضائي بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، فالضبط إذن يعد أيضا إجراء من إجراءات التحقيق في الجرائم المعلوماتية؛ بوضع اليد على الشيء وحبسه والمحافظة عليه، للحصول علىدليل لمصلحة التحقيق عن طريق إثبات واقعة معينة[2]، وهو ما سنبرزه فيما يلي:

أولا: تفتيش نظم المعلوماتية

عملية تفتيش تنصب على المكونات المادية بأوعيتها المختلفة، للبحث في أي شيء يتصل بجريمة معلوماتية ما للكشف عنها، يدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات، هي:

الحالة الأولى: في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات.

الحالة الثانية: إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن، ففي ألمانيا يرى الفقه [3]، أنه يمكن أن يمتد

---

(١) طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1 ، ٢٠١١-٢٠١٢، ص ١٣١.

(٢) يمثل الحاسوب الآلي المحل الرئيسي للتفتيش في نظم المعلوماتية، وينصب التفتيش على المكونات المادية: وهي مجموعة من الوحدات لكل منها وظيفة محددة وتتصل مع بعضها البعض بشكل يجعلها تعمل كنظام متكامل، وتسمى بمعدات الحاسوب وهي: وحدات الإدخال، وحدة الذاكرة الرئيسية، وحدة ذاكرة القراءة، وحدة الحاسوب والمنطق، الشاشة، وحدة التحكم، وحدة الذاكرة المساعدة، وحدة الإخراج، الطابعة.

أنظر : طارق الدسوقي عطية، المرجع السابق، ص441 .

(٣) طرشي نورة، المرجع السابق، ص ١١٥.

التفتيش إلى سجلات البيانات التي تكون في موقع آخر تطبيقا لمقتضيات القسم 103 من قانون الإجراءات الجزائية الألماني، وذلك عندما يكون مكان تخزين البيانات الفعلي خارج المكان الذي يتم فيه التفتيش.

إذن لتفتيش الحاسوبات الآلية ذات نهاية طرفية في دولة أجنبية، نصت بعض التشريعات على طريقة ثانية كإجراء للتحقيق في الجريمة المعلوماتية وهذه الطريقة هي: التنصت والمراقبة الالكترونية لشبكات الحاسوب ويقصد بهذه الطريقة -التنصت- مراقبة المحادثات التلفونية وتسجيلها بالنسبة للأحاديث الخاصة بشخص أو أكثر مشتبه فيه، ويعتقد بفائدة محادثته في الكشف عن الجريمة، وذلك عن طريق إخضاعها لنوع من الرقابة بقصد التعرف على مضمونها.

وقد حذا المشرع الجزائري حذو معظم التشريعات المعاصرة، بأن قرر المادة 65 مكرر5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا اقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بإعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور.

الحالة الثالثة: إذا وجدت مكونات الحاسوب المادية (في حالة الحاسوبات الآلية المحمولة) في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة... الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات، وقد اتفقت بعض التشريعات، كالتشريع الجنائي الكندي في المادة 487 التي أجازت إصدار أمر قضائي لتفتيش وضبط أي شيء يؤدي للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها، ونصت صراحة على إمكانية تفتيش مكونات الحاسوبات المادية للكشف عن الجريمة المعلوماتية باتخاذ أي إجراء أو القيام بأي فعل لازم لجمع الأدلة والحفاظ عليها[1].

ثانيا: **تفتيش نظم الحاسوب المنطقية أو المعنوية**: يعرف الكيان المنطقي للحاسوب بأنه: " مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات"[2].

وهو يشتمل على جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي كالبرامج ونظم التشغيل وقواعد البيانات ... الخ، لقد ثار الخلاف في التشريع المقارن في مسألة ضبط وتفتيش المكونات المعنوية أو المنطقية للحاسوب، فتعددت الآراء في هذا الشأن؛ فذهب رأي إلى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة، فإن هذا المفهوم يجب أن يمتد ليشمل البيانات الالكترونية، كالقانون الإجرائي اليوناني في نص المادة 251 التي تعطي لسلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل، تفسيرا لعبارة أي شيء بأنها تشمل ضبط البيانات المخزنة أو المعالجة آليا أو الكترونيا، بما فيها ضبط البيانات المخزنة في حاملات البيانات المادية، أو في الذاكرة الداخلية وذلك بإعطاء المحقق أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل للمحاكمة الجنائية، على أساس إنها كيانات يمكن قياسها بما انها نبضات أو ذبذبات الكترونية قابلة لان تسجل وتخزن على وسائط معينة يمكن قياسها[3].

وقد حذا المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري حذو التشريعات السابقة بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة

---

[1] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص385 .

[2] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، 2007.

[3] هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية القاهرة،2000، ص 52.

الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك".

هناك بعض الحالات الخاصة يفرض التساؤل عن كيفيات التعامل معها قانونيا في إجراءات ضبط المعلوماتية، والتي سنرى كيف تصدت لها القوانين المقارنة، بالحل كالتالي:

• مدى جواز الاطلاع على المحتويات المعلوماتية:

يطرح في مجال التفتيش والضبط المعلوماتي في الجريمة المعلوماتية إشكال جواز أو عدم جواز اطلاع مأمور الضبط القضائي على المحتويات المعلوماتية، فجرى العمل في ألمانيا على أن سلطة الاطلاع على مطبوعات الحاسوب وحاملات البيانات تقتصر على المدعى العام فقط، ولا يكون لضبط الشرطة الحق في قراءة البيانات عن طريق تشغيل البرامج أو الوصول إلى البيانات المخزونة دون إذن من الشخص الذي له الحق في نقل هذه البيانات، لكن كل ما يمكنهم هو مجرد فحص حاملات البيانات دون استخدام أي مساعدات فنية تطبيقا لما جاء في القسم 110 من قانون الإجراءات الألماني [1].

• حق المتهم في الصمت:

يقصد بالحق في الصمت أن للشخص المتهم في جريمة ما مطلق الحرية في الكلام أو عدمه أو عدم الإجابة على الأسئلة الموجهة إليه من قبل مأمور الضبط القضائي أو الموظف القائم بالتحقيق معه، لأنه غير ملزم بالكلام كما يجب أن يراعى أن رفضه الإجابة وصمته، لا يجوز أن يؤخذان كقرينة ضده[2]، وذلك تطبيقا للقاعدة الإجرائية العامة التي مفادها: "عدم إجبار الشخص على الكلام أمام أي جهة أو سلطة كحق من حقوق الإنسان". والتي أوصى بها كل من المؤتمر الدولي السادس لقانون العقوبات المنعقد في روما سنة 1953، والمؤتمر الدولي الذي نظمته اللجنة الدولية لرجال القانون في أثينا في جوان لعام 1955، كما حرصت معظم التشريعات الجنائية على النص صراحة على هذا الحق كالقانون الفرنسي في المادة 114 قانون إجراءات جزائية التي تلزم قاضي التحقيق أن ينبه المتهم عند حضوره أمامه لأول مرة إلى أنه حر في عدم الإدلاء بأي إقرار، ويثبت ذلك التنبيه في محضر التحقيق، ومثلما فعل المشرع الجزائري في المادة 100 من قانون الإجراءات الجزائية.

أما بالنسبة للشاهد المعلوماتي، نعلم أن الشهادة هي إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص عما شهده أو سمعه أو أدركه بحواسه عن هذه الواقعة، كما يقصد بسماع الشهود السماح لغير أطراف الدعوى الجنائية بالإدلاء بما لديهم من معلومات أمام سلطات التحقيق، والشاهد المعلوماتي قد يكون شاهدا عاديا أو خبيرا في الدعوى القائمة، بالنسبة للشاهد العادي فهو ذلك الشخص الذي يقدم إلى القاضي معلومات حصل عليها بالملاحظة الحسية، أما الخبير فهو ذلك الشخص المختص الذي يقدم إلى القاضي تقارير وآراء توصل إليها بتطبيق قوانين علمية وأصول فنية.

▪ مدى جواز إجبار المتهم والشاهد المعلوماتي على الإدلاء ببيانات

بالنسبة للمتهم المعلوماتي جرى العمل في الفقه والقانون في فرنسا حسب نص المادة 27 من ق اج ج الفرنسي التي نصت على أنه من غير الممكن إجراء تفتيش المساكن وضبط الأشياء التي يمكن أن تكون متعلقة بالجريمة إلا بموافقة صريحة

---

[1] طرشي نورة، المرجع السابق، ص ١٢٠.

[2] سامي صادق الملا، اعتراف المتهم، دار الفكر العربي، الطبعة الأولى، ١٩٩٨، ص 187 وما بعدها.

وأيضا: طارق الدسوقي عطية، المرجع السابق، ص459 .

للشخص المراد تفتيش منزله أو أشيائه كما بينت الفقرة الثانية من نفس المادة، بأن الموافقة يجب أن تكون صريحة لا ضمنية، وفي حالة رفض الموافقة الصريحة فإن ذلك يعني رفض ذوي الشأن، ولذلك تعد الإجراءات باطلة وعلى هذا لا يجوز قانونا إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات أو إلزامه بالكشف عن الشفرات أو كلمات السر خاصة بالدخول إلى هذه المعلومات أو إجباره على تقديم الأمر اللازم لوقف فيروس، تطبيقا لمبدأ عدم جواز إلزام الشخص بتقديم دليل ضد نفسه سواء عن طريق الشهادة أو غيرها من عناصر الإثبات، إلا أن ذلك لا يمنع من إجباره على تسليم الشفرة الخاصة بالحاسوب الآلي المخزنة فيه البيانات محل الجريمة[1].

والشاهد المعلوماتي بنوعيه المذكورين سابقا يلتزم بالكشف عن الشفرات أو كلمات السر التي يكون على علم بها، كما أنه يلتزم في بعض الدول الأوروبية بإجراء ما يسمى بإنعاش الذاكرة، بفحص الأماكن والمستندات التي توجد تحت سيطرته وذلك في كل من السويد وفنلندا والنرويج، أما في انجلترا فالقانون الانجليزي الصادر عام 1984 يعطي المحققين الحق في إلزام الغير بتمكين سلطات التحقيق الدخول إلى المعلومات المخزنة في الحاسوب الآلي أو الاطلاع عليها أو قراءتها، كما تسمح بعض التشريعات المقارنة في مجال التحقيق المعلوماتي الاستفادة من الشهود كخبراء أو كمساعدين للقضاء من تلقاء أنفسهم ودون حاجة لاستدعائهم[2].

ثالثا: القواعد الشكلية لتفتيش نظم المعلوماتية

تتلخص هذه القواعد كما يلي:

أ -**إجراء التفتيش بحضور أشخاص معينين بالقانون**: من بين هذه الأشخاص: المهم والقائم بالتفتيش وشاهدين طبقا للمادة 45 من قانون الإجراءات الجزائية الجزائري، تنص على أن: أن التفتيش يتم بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية-القائم بالتفتيش-، وإذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته، غير أنه كاستثناء على هذه القواعد نص المشرع الجزائري في الفقرة الأخيرة من المادة 45 من قانون الإجراءات الجزائية الجزائري، على أنه: "لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات."

ب -**إعداد محضر خاص بالتفتيش**: ويكون بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضرا خاصا بالتفتيش والضبط، تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة وحرص.

ت -**إجراءات تنفيذ تفتيش نظم الحاسوب الآلي وميعاده:** لهذه الإجراءات خصوصية تتميز بها، وذلك لدقة التعامل مع الأجهزة والبرامج الموجودة عليها، ولكي تتم على أكمل وجه، يجب تحديد نوع النظام المراد تفتيشه، وبالتالي يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها، والاستعانة بخبراء النظام للاستعانة بهم في عملية إجراء التفتيش، ومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ومعرفة مكان القيام بتحليل نظم الحاسوب الآلي[3].

---

[1] أنظر: جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001، ص 106 .

[2] محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة، ط 8، 2008، ص.68 .

[3] طرشي نورة، المرجع السابق، ١٢٥.

بالإضافة إلى تحديد هوية أعضاء فريق التفتيش يجب على القائم بالتفتيش اتخاذ الخطوات التالية عند تنفيذ إذن التفتيش والتي تتلخص في ما يلي:

- تأمين حماية مسرح الجريمة، بضمان فصل القوة الكهربائية عن موقع المعاينة وأجهزة خدمة شبكة الانترنت، لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على أثار الجريمة.
- إبعاد المتهم عن مكان النظام إن كان قريبا منه .
- أخذ الحيطة لمنع تمكن المتهم من الدخول عن بعد للنظام المعلوماتي .
- الدخول إلى الموقع ببطء، لكي لا يتم تشويه أو إتلاف الدليل .
- عدم لمس لوحة المفاتيح، لأن ذلك قد يستلزم استخدام برامج أخرى احتيالية أو صعبة.
- يجب العناية بالملاحظات وكلمات السر ورموز الشفرة إلى غيرها من العمليات والإجراءات الفنية التي تساعد على الكشف عن الجريمة المراد إثباتها[1] .

وفي نطاق تفتيش نظم الحاسوب، نجد أن أغلب التشريعات الإجرائية لم تحدد مدة معينة لتنفيذ إجراء التفتيش ما عدا البعض منها كالتشريع الانجليزي الذي حدد مهلة الشهر الواحد من تاريخ إصدار الإذن كما أنها تختلف في الزمن الذي يجري فيه التفتيش أو تحديد المدة التي يجري فيها، غير أن الرأي الغالب في مجال تفتيش النظم المعلوماتية هو عدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر فيه الجرائم المعلوماتية هو ليلا، لسهولة الاتصال ومجانيته في ذلك الوقت في بعض الحالات، وأيضا لسهولة الدخول إلى المواقع المستهدفة بالفعل الإجرامي لقلة المستخدمين في هذا الوقت، مثلما فعل المشرع الجزائري في الفقرة الثالثة من المادة 47 من ق إ ج ج[2].

المبحث الثاني: إجراءات التحري المستحدثة للكشف عن الجرائم المعلوماتية

تعتبر الضبطية القضائية صاحبة الاختصاص الأصيل في الكشف أو في التحري عن الجرائم عموما، وفي سبيل كشفها عن هذه الجرائم، أعطاها القانون سلطة التحري عن الجرائم، كما منحهم قانون الوقاية من الفساد ومكافحته ولئذا قانون الإجراءات الجزائية الجديد أساليب جديدة للتحري، أسماها "أساليب التحري الخاصة"، كما أضافت التأكيد على اعتبار جرائم المساس بأنظمة المعالجة الآلية للمعطيات من الجرائم التي قرر المشرع صراحة وبنص صريح إمكانية إتباع إجراءات التحري الخاصة في الكشف عنها ومكافحتها، نص المادة٠٤ من القانون٠٩-٠٤ المؤرخ في٥ أوت٢٠٠٩ يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، التي قررت الفقرة الثانية منها أنه: " في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني".

أول خطوة في الكشف عن جرائم الإعلام الآلي على مستوى الضبطية القضائية هي مرحلة التحري، حيث يقصد بالتحري في مجال الضبط القضائي، البحث عن الجرائم المرتكبة والتحقق من صحة الوقائع المبلغة لضباط الشرطة

---

[1] عفيفي كامل عفيفي، المرجع السابق، ص65 .

(٢) طرشي نورة، المرجع السابق، ص ١٢٦.

القضائية، وجمع القرائن التي تفيد في حصول الواقعة أو نفي وقوعها[1]، لذلك فإن رجال الضبطية القضائية إذا أخطروا بجريمة من الجرائم، فإنهم يقومون بالإجراءات الأولية وهذه الإجراءات مرتبطة بالبحث والتحري والذي يعد كمرحلة تمهيدية للدعوى، هذه الإجراءات في حد ذاتها ضرورية، فكلما قرب الزمن بين الإجراء والجريمة كانت الأدلة واضحةً أكثر وأسلم ولم يشبها أي تغيير أو تحريف ومن تم كانت أدعى للثقة[2]، وفي سبيل مكافحة جرائم الفساد، نص المشرع على مجموعة من أساليب التحري تضاف إلى تلك الأساليب التقليدية، وأطلق على هذه الأساليب عبارة "أساليب التحري الخاصة"، ويتمثل الهدف من هذه الأساليب في الكشف عن هذه الجرائم واستئصال الفساد وردع المفسدين.

المطلب الأول: توسيع الإجراءات الخاصة بالاختصاص في الجرائم المعلوماتية

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه تطويقها والقضاء عليها أو على الأقل الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث وضع قواعد وأحكام خاصة لسلطة التحري والمتابعة الغرض منها هو مواجهتها، وقد وردت هذه الأساليب في قانون الإجراءات الجزائية المعدل والمتمم بموجب القانون٢٢/٠٦ الصادر في٢٠/١٢/٢٠٠٦، وقانون الوقاية من الفساد ومكافحته رقم٠١/٠٦ المؤرخ في٢٠ فيفري٢٠٠٦، وهي: أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وكذلك أسلوب التسرب أو كما سماه قانون الوقاية من الفساد ومكافحته أسلوب الاختراق.

لذلك لابد من شرح هذه الأساليب، وكيف يمكن التوفيق بين هذه الأساليب التي تتم خلسة وما تحمله من معنى الاعتداء على الحريات والحقوق الخاصة للأفراد، خاصة إذا علمنا أن الحرية الخاصة للأفراد وسرية المراسلات مضمونة دستوريا[3].

الفرع الأول: جواز تمديد الاختصاص المحلي والنوعي الدولي للمحاكم الجزائرية: حيث نصت المادة 329 من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05).

كما أنشئت الأقطاب القضائية الجزائية المتخصصة بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية من بين الجرائم التي تختص بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (المواد37 و 40 و329 من قانون الإجراءات الجزائية).

كذلك، نظم المشرع الجزائري في القانون رقم٠٤/٠٩ المؤرخ في٥ أوت٢٠٠٩، أحكاما جديدة خاصة بالاختصاص في مجال بالجريمة المعلوماتية تتماشى والتطور الذي لحق الجريمة، من هذه القواعد ما نصت عليه المادة الثالثة التي تضمنت الإجراءات الجديدة التي تتطلبها التحريات والتحقيقات من ترتيبات تقنية، بالإضافة إلى ذلك، قررت المادة١٥ من القانون ٠٤/٠٩ أنه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في

---

(١) محمد ماجد ياقوت، أصول التحقيق الإداري في المخالفات التأديبية، دراسة مقارنة، منشأة المعارف، الإسكندرية، مصر، بدون سنة نشر، ص ٢٨٩.

(٢) محدة محمد، ضمانات المتهم أثناء التحقيق، الجزء الثالث، الطبعة الأولى، دار الهدى، عين مليلة، الجزائر، ص ١٠٥.

(٣) المادة (٣٩) من الدستور الجزائري لعام ١٩٩٦، معدل ومتمم، التي تنص على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا، وتستهدف مؤسسات الدولة الجزائرية والدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

الفرع الثاني: توسيع مجال اختصاص النيابة العامة

بموجب المادة 37 من قانون الإجراءات الجزائية، تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها بها من قبل، حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

كذلك سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، إذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون، بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر و١٤٤ مكرر1 و144 مكرر٢ من قانون العقوبات المعدل والمتمم بالقانون رقم٠١/٠٩ المؤرخ في 26 يونيو2001[1].

المطلب الثاني: الإجراءات المتعلقة بالتحري والكشف عن الجريمة المعلوماتية

إضافة لما سبق ودائما في إطار المكافحة الإجرائية للجرائم المعلوماتية تم توسيع مجال اختصاص النيابة العامة في مجال البحث والتحري عن هذه الجرائم بمنح الإذن بالتفتيش والقيام باعتراض المراسلات وتسجيل الأصوات والتقاط الصور حسب نص المادة 65 مكرر 5 في إطار تعديل من قانون الإجراءات الجزائية الجزائري بالقانون٠٦/٢٢ المؤرخ في2006/12/20 التي تنص: "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية، أن يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون، وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.

الفرع الأول: الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور

مكن المشرع الجزائي ضابط الشرطة القضائية من صلاحية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور للكشف عن الجرائم المعلوماتية، وهي إجراءات تباشر بشكل خفي، على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة[2].

---

[1] طرشي نورة، المرجع السابق، ص ١٣٤.

[2] خلفي عبد الرحمن، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة، الجزائر، ٢٠١٠، ص ٧٢- ٧٣.

وإلتقاط الصور يكون بالتقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص، ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن العامة والخاصة.

أما تسجيل الأصوات، فيتم عن طريق وضع رقابة على الهواتف وتسجيل الأحاديث التي تتم عن طريقها، كما يتم أيضا عن طريق وضع ميكروفونات حساسة تستطيع إلتقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضا عن طريق التقاط إشارات لاسلكية أو إذاعية[1].

إن ما يهم هو أن مثل هذا الإجراءات يمكن له المساس بالحرية الشخصية، خصوصا إذا علمنا أن سرية المراسلات هي حق دستوري، فقد جاء في المادة٠٣ من القانون رقم٠٩-٠٤ المؤرخ في ٥ أوت٢٠٠٩ يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2]، أنه: "مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية[3].

بالإضافة إلى أن كل متهم بريء حتى تثبت إدانته[4]، لذلك هل يجوز إثبات أو نفي الاتهام عن المشتبه فيه، باللجوء إلى وسيلة التسجيل الصوتي أو اعتراض المراسلات أو التقاط الصور في الأماكن العامة والخاصة، وخصوصا أن مثل هذه الإجراءات أو الوسائل قد لا تمس بشخص المتهم فقط، وإنما كذلك بمن يحيطون به من أقاربه أو معارفه؟.

يفرق الفقه بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، فبينما يكون الأول دون رضا المعني، يكون الثاني برضا أو بطلب من صاحب الشأن، ويخضع لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك.

ويعد هذا الإجراء الحديث من أهم إجراءات التحقيق، مكن المشرع ضابط الشرطة القضائية ممارسته للكشف عن الجرائم التي حددها على سبيل الحصر في المادة٦٥ مكرر٥ بموجب قانون الإجراءات الجزائية، تباشره الجهة القضائية في بعض الجنايات والجنح التي وقعت أو التي قد تقع في القريب العاجل، بمعنى أنها إجراء للتحري والتحقيق، وكل ما يتمخض عنها كدليل ضد كل شخص قامت تحريات جدية على أنه ضالع في ارتكاب هذه الجريمة أو لديه أدلة تتعلق بها، وأن في مراقبة أحاديثه الهاتفية ما يفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية.

لكن مع ذلك، نجد المشرع حاول يوفق بين هذه المتعارضات، بأن أجاز هذه الأساليب، ولكن بضوابط وهي مباشرة التحري بإذن من وكيل الجمهورية المختص، وإلتزام أعوان وضباط الشرطة القضائية القائمين بالإجراء السر المهني، وفيما

---

(١) حسن صادق المرصفاوي، المرصفاوي في التحقيق الجنائي، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر، ١٩٩٠، ص ٧٨.

(٢) يقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال في إطار المادة ٢ /أ من القانون رقم ٠٤/٠٩ المؤرخ في ٥ أوت ٢٠٠٩ يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

(٣) يقصد بالمعطيات المعلوماتية في إطار المادة ٢ / ج من القانون رقم ٠٤/٠٩ المؤرخ في ٥ أوت ٢٠٠٩ يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها .

(٤) تنص المادة (٤٥) من دستور عام ١٩٩٦ على أنه: "كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية إدانته مع كل الضمانات التي يتطلبها القانون."

يلي نتولى شرح كلا الضابطين، فالمشرع على الرغم من إقراره أساليب تحري خاصة قد تمس بحرمة الحياة الخاصة إلا أنه يعاقب على اللجوء لاستعمالها بطرق غير مشروعة[1]، وهو ما سنشير إليه على النحو التالي:

أولا- مباشرة التحري بإذن من وكيل الجمهورية

لم يسمح المشرع بإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلا بإذن من وكيل الجمهورية المختص، وتباشر هذه العمليات تحت مراقبته، وهذا ما قررته المادة٤ ٠ من القانون٩ ٤٠ ٠ التي جاء فيها أنه: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة".

ويجب أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سواء أكانت سكنية أو غير سكنية، كما يجب أن يتضمن نوع الجريمة التي تبرر اللجوء إلى هذه التدابير ومدة هذه التدابير[2]، لذلك فإن الإذن المسلم من قبل وكيل الجمهورية للتحقيق في جريمة ما لا يصلح للتحقيق في جريمة أخرى، إلا بإذن جديد، كذلك يجب أن يتضمن الإذن كل الأماكن التي توضع فيها الترتيبات التقنية من أجل التقاط وتسجيل وتثبيت الكلام المتفوه به بصفة خاصة من شخص أو عدة أشخاص[3].

وعند مباشرة التحريات والتحقيقات، يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص، محضر عن كل عملية اعتراض للمراسلات وتسجيل الأصوات والتقاط للصور، وحتى عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتسجيل الصوتي أو السمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها[4]، بحيث يشتمل المحضر على كل البيانات المذكورة سابقا وتكون محددة تحديدا نافيا للجهالة، ويجب أن يشتمل المحضر على توقيع محرره في نهايته[5]، بعد أن يصنف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب، المراسلات أو الصور أو المحادثات المسجلة أو المفيدة في إظهار الحقيقة في محضر يودع بملف المتهم، وتنسخ وتترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض[6].

ثانيا- إلتزام السر المهني

تكون إجراءات التحري والتحقيق سرية، ومن ثم، فإن بحثها ضمن الضمانات الممنوحة للمتهم[7]، والسرية تعني القيام قدر الإمكان ممن هو قائم بالتحري أو كلف بإجراء من إجراءاته أو ساهم فيه بالمحافظة على السر المهني، وبالتالي صارت السرية ليس هدفها كما كان عليه من قبل هو تسهيل قمع المتهم، بل صارت وسيلة لضمان الحريات الشخصية[1].

---

[١] المادة (٣٠٣ مكرر) من الأمر رقم ١٥٦/٦٦ معدلة ومتممة بموجب المادة (٣٣) من القانون رقم ٢٣/٠٦ المؤرخ في ٢٠ ديسمبر ٢٠٠٦.

[٢] المادة (٦٥ مكرر ٧) الأمر رقم ١٥٥/٦٦ المعدل والمتمم بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

[٣] المادة (٦٥ مكرر ٧) الأمر رقم ١٥٥/٦٦ المعدل والمتمم بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

[٤] المادة (٦٥ مكرر ٩) الأمر رقم ١٥٥/٦٦ المعدل والمتمم بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

[٥] كمال كمال الرخاوي، إذن التفتيش فقها وقضاء، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، ٢٠٠٠، ص ٢٧١.

[٦] المادة (٦٥ مكرر ١٠) الأمر رقم ١٥٥/٦٦ المعدل والمتمم بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

[٧] المادة (١١) من الأمر رقم ١٥٥/٦٦ المعدل والمتمم بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

فقد نص المشرع صراحة على أن هذه العمليات تتم بمراعاة السر المهني ودون المساس به[2]، فالضابط المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ملزم قانونا بكتمان السر المهني ويجب أن يتخذ مقدما التدابير اللازمة لضمان احترام ذلك السر[3]، وقد نص قانون الإجراءات الجزائية على أن تكون إجراءات التحري والتحقيق سرية[4]، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع، وكل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها فيه، لذلك فعملية التحري عن جرائم المساس بأنظمة المعالجة الألية للمعطيات تتم بسرية مطلقة، فيمنع منعا باتا أن يخبر المشتبه فيه بهذه التحريات أو أي شخص آخر، كذلك يمنع على ضابط الشرطة المأذون له أو المناب أن يفصح عن مضمون محضر التحريات لأي شخص كان، وإلا وقع تحت طائلة الجزاء الجنائي بتهمة إفشاء السر المهني، فيجب على ضباط الشرطة القضائية ومرؤوسيهم عدم إفشاء الأسرار التي جمعوها أثناء التحريات، لأن سمعة المواطنين لا يجوز أن تظل مهددة ببيانات غير مؤكدة[5].

الفرع الثاني: أسلوب التسرب أو الاختراق

يعتبر التسرب تقنية جديدة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة ٢٠٠٦، عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة ٦٥ مكرر٥)، كما يجوز لوكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن شروط محددة[6] ويشترط حصول الضابط المكلف بالتسرب على الإذن من وكيل الجمهورية المختص، ويجب أن تتم العملية تحت أشرافه ومراقبته، فإن قرر قاضي التحقيق مباشرة هذا الإجراء وجب عليه أولا إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح الإذن مكتوب لضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه[7]، وهذا تحت طائلة البطلان المطلق، فيجب أن يكون الإذن مكتوبا يتضمن كل ما يتعلق بعملية التسرب وكذلك هوية ضباط وأعوان الشرطة المأذون لهم بالتسرب.

والتسرب هو قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيهم، بإيهامهم أنه فاعل معهم أو شريك لهم [8]، فالتسرب إذن هو قيام المأذون له بالتحقيق في الجريمة بمراقبة الأشخاص المشتبه في ارتكابهم جريمة، أو التوغل داخل جماعة إجرامية بإيهامهم أنه شريك لهم، ويسمح لضباط وأعوان الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة بعض

---

(١) سهيلة بوزبرة، مواجهة الصفقات العمومية المشبوهة، مذكرة ماجستير في القانون الخاص، كلية الحقوق جامعة ج يجل، ٢٠٠٨، ص ١٢٧.

(٢) المادة (٦٥ مكرر ٧) الأمر رقم ١٥٥/٦٦ المعدل والمتمم بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

(٣) المادة (٤٥ /٣) من الأمر رقم ١٥٥/٦٦ المعدل والمتمم بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

(٤) المادة (١١) الأمر رقم ١٥٥/٦٦ معدل ومتمم.

(٥) قدري عبد الفتاح السهاوي، المرجع السابق، ص ١٩١.

(٦) المادة (٦٥ مكرر ١١) الأمر رقم ١٥٥/٦٦ المعدل والمتمم بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

(٧) محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية، الجزائر، ٢٠٠٩، ص ١١٥.

(٨) المادة (٦٥ مكرر ١٢) الأمر رقم ١٥٥/٦٦ المعدل والمتمم بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

الجرائم، دون أن يكون مسؤولا جزائيا[1]، وذلك بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، بإخفاء الهوية الحقيقية[2].

ولهذا يجوز لضابط أو عون الشرطة القضائية المرخص له بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض، دون أن يكونوا مسؤولين جزائيا القيام بما يلي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم، الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخريب أو الإيواء أو الحفظ أو الاتصال[3].

ويحظر على المتسرب إظهار الهوية الحقيقية في أي مرحلة من مراحل الإجراءات مهما كانت الأسباب إلا لرؤسائهم السلميين، لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعريض العضو المكشوف عن هويته للخطر، وهو ما أكده المشرع بموجب المادة٦٥ مكرر١٦) بأن نصت صراحة أنه:" لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات".

كما عاقب المشرع كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة من٥٠٠٠ دج إلى٢٠٠٠٠ دج، وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، فتكون العقوبة الحبس من خمس سنوات إلى١٠ سنوات والغرامة من٢٠٠٠ دج إلى٥٠٠٠ دج، وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من١٠ إلى٢٠ سنة والغرامة من٥٠٠٠ إلى١٠٠٠٠ دج[4].

ولضمان نجاح عملية التسرب للكشف عن جرائم الصفقات العمومية، يلتزم المتسرب القيام بهذه العملية بكل الإجراءات المحددة قانونا، وأهمها حصوله على الإذن المكتوب من قبل وكيل الجمهورية المختص بحيث إلتزام هذا الأخير بالإشراف والمراقبة على نجاح العملية، وكما يلتزم المتسرب حفاظا على أمنه وسلامة العملية بعدم الكشف عن هويته، وذلك لخطورة مهمته التي تتطلب جرأة وكفاءة ودقة في العمل.

ورغم أن المشرع أجاز مثل هذه الأفعال التي تعتبر في حقيقة الأمر جرائم من أجل خلق الثقة وتعزيزها في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم والنجاح في إيهامهم بأنهم شركاء أو فاعلون، مع ذلك منع المشرع هؤلاء الضباط أو الأعوان من أن يحرّضوا المشتبه فيهم على ارتكاب الجريمة، بمعنى أنه يمنع على الضباط والأعوان المتسربين أن يخلقوا الفكرة الإجرامية للشخص الموضوع تحت المراقبة ودفعه لارتكاب الجريمة، فهذا الفعل ممنوع تحت طائلة بطلان الإجراء.

---

[1] عيساوي نبيلة، المرجع السابق، ص ٠٢.

[2] عبد الرحمن خلفي، المرجع السابق، ص ٧٤- ٧٥.

[3] المادة (٦٥ مكرر ١٤) من الأمر رقم ١٥٥/٦٦ المعدل والمتمم بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

[4] المادة (٦٥/٣ – ٤ مكرر) من الأمر رقم ١٥٥/٦٦ المعدل والمتمم ومعدل بموجب المادة (١٤) من القانون رقم ٢٢/٠٦.

المطلب الثاني: إجراءات التحري والحجز والكشف عن الجرائم المعلوماتية بموجب القانون 09/04

بين القانون 09/04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إجراءات مراقبة الاتصالات الإلكترونية، وتفتيش وحجز المنظومة المعلوماتية، وعليه سنوجزها كالتالي:

الفرع الأول: مراقبة الاتصالات الإلكترونية وتجميعها

القاعدة أنه أضفى المشرع الجزائري الحماية القانونية للبيانات ذات الطابع الشخصي من خلال أسمى نص في النظام القانوني الجزائري ، ألا وهو الدستور، وهذا في إطار القواعد العامة التي ت عنى بالحماية القانونية للحياة الخاصة للأفراد ، وهو ما ينطوي عليه بالضرورة حماية بياناتهم الشخصية من المعالجة الآلية، بحيث اعترف المشرع الدستوري الجزائري بها في المادة 77 التي تنص على أنه: "يمارس كل واحد جميع حرياته، في إطار احترام الحقوق المعترف بها للغير في الدستور، لاسيما احترام الحق في الشرف، وستر الحياة الخاصة."...

كما أيدت ذلك المادة 46 من دستور سنة 1996 التي نصت على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"، إلا أنه في تعديل الدستوري لسنة 2016، حاول المشرع مواكبة التطور الذي يشهده العالم في مجال حماية البيانات الشخصية، من خلال إضافة فقرتين للمادة أعلاه تنصان على أنه ":لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون انتهاك هذا الحكم[1].

إن أضافت الفقرتين الثالثة والرابعة في التعديل الأخير، إنما ينم عن اقتناع المشرع الجزائري بضرورة المبادرة إلى وضع الآليات القانونية الكفيلة بحماية البيانات الخاصة بالأشخاص الطبيعيين خلال عملية المعالجة الآلية لها، كما يدل الإقرار الدستوري على أن القانون الخاص بالحماية البيانات هو مسألة وقت فقط، خاصة في ظل النشاط التشريعي الذي الجزائر في العشرية الأخيرة، وأن وزارة البريد وتكنولوجيات الإعلام والاتصال تدرس ابتداء من نوفمبر 2014 مشروع قانون حول حماية البيانات الشخصية على الأنترنيت والذي يفترض أن يصدر قريبا.

علما أن الجزائري هو الوحيد بين الدساتير العربية الذي تطرق لحرمة البيانات الخاصة من المعالجة الإلكترونية، بحيث تكتفي جلها بتكريس الحماية الدستورية للمراسلات بكل أشكالها فقط[2].

وبهذايكون المشرع الجزائري رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها، قد خول استثناء السلطة القضائية وفي إطار قرار معلل بأن تتبع إجراءات تمس البيانات الشخصية، بالنظر لخطورة بعض الجرائم المعلوماتية المحددة حصرا: تسجيل الاتصالات الإلكترونية في حينها.

كما بين القانون 09/04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مادته الرابعة، الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية، وذلك على سبيل الحصر، وهذه الحالات هي:

---

[1] القانون رقم 01 – 16 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14 ، الصادرة في 07 مارس 2016 .

[2] لوكال مريم، الحماية القانونية للبيانات ذات الطابع الشخصي في العالم الرقمي ، بالملتقى الوطني الموسوم بـ: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي ٧ و٨ فبراير ٢٠١٧، ص ٦.

• للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

• في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

• لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الإلكترونية.

يظهر من خلال استقراء نص هذه المادة، أن المشرع الجزائري يحاول الاستفادة بدوره من التطور التكنولوجي والمميزات التي يخولها، من خلال وضع المشتبهين فيهم تحت المراقبة الإلكترونية، وهي على عكس المراقبة الشخصية أقل تكلفة من حيث الوقت والمال والمخاطر الأمنية إضافة إلى فعاليتها، إلا أنه من جهة أخرى، فإن وضع الشخص تحت المراقبة الإلكترونية سواء ما تعلق باتصالاته الهاتفية أو نشاطاته عبر الأنترنيت، من شأنه انتهاك حرمة البيانات ذات الطابع الشخصي له، باعتبار أنه لدواعي فرز المعلومة للتأكد من قيمتها كدليل إثبات أو نفي، يستدعي سماعها أو قراءتها بكل تأني، وهذا ما من شأنه الوصول إما لأنها معلومة ضرورية لاستكمال التحقيقات، أو أنها معلومات شخصية لا دخل لها بالقضية، كما يمكن أن يصار إلى تبرئة الشخص تماما، لكن بعد ماذا؟.

بغرض تأطير هذه العملية الحساسة وتخفيف تأثيراتها السلبية على حماية الحياة الخاصة للأفراد وضع المشرع عدة ضمانات هي:

1 -**حصر الحالات التي يمكن اللجوء فيها إلى المراقبة الإلكترونية**

هي الحالات التي أوضحتها المادة الرابعة من القانون٠٩-٠٤ على سبيل الحصر":

أ- للوقاية من الأفعال الموصوفة بالجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة- .

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني- أو مؤسسات الدولة أو الاقتصاد الوطني.

ج- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون- اللجوء إلى المراقبة الإلكترونية.

د- في إطار تنفيذ المساعدة القضائية الدولية المتبادلة."[1]

بإستقراء الحالات هذه، نجد أن المشرع ق لص من الحالات التي يمكن فيها اللجوء إلى عملية المراقبة الإلكترونية وحصرها في الجرائم التي تمس الأمن الوطني، ذلك أنه عندما يتعلق الأمر مثلا بالجرائم الإرهابية والتي تطال المدنيين فإنه لا يمكن الحديث عن حقوق الإنسان، وكذا في حالات تنفيذ المساعدة القضائية، إلا أن إضافة الحالة" ج" والتي تعني إمكانية اللجوء في كل قضية مستعصية إلى المراقبة الإلكترونية صغيرة كانت أو كبيرة، يؤدي إلى تعميم استخدام الآلية دون حد.

---

[1] لوكال مريم، المرجع السابق، ص ٠٩.

2 -**وضع آلية إقرار المراقبة الإلكترونية تحت سلطة القضاء:**

تضيف المادة 4/2 من القانون٠٩-٠٤، بأنه":لا يجوز إجراء عمليات المراقبة، إلا بإذن مكتوب من السلطات القضائية المختصة."

كما أنه عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية، إذنا لمدة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها [1].

كما تنص المادة 41 من المرسوم الرئاسي رقم١٥/٢٦١ المؤرخ في 08 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]، على أن الهيئة تمارس اختصاصاتها الحصرية في مجال مراقبة الاتصالات الإلكترونية تحت مراقبة قاض مختص.

كما يخضع الموظفون الذين يدعون إلى الاطلاع على معلومات سرية إلى أداء اليمين أمام المجلس القضائي قبل تنصيبهم، وهم يلزمون بذلك بالسر المهني(المادتين 27 و28 المرسوم الرئاسي١٥/٢٦١) .

يعتبر وضع هكذا آلية تمس بالحريات الفردية والحياة الخاصة للأفراد تحت يد القضاء المستقل، ضمانة حقيقية باعتبار أن القاضي يهدف إلى الموازنة بين ضرورات التحقيق وإلزامية حماية الأفراد المشتبه فيهم، فمجرد الاشتباه لا يجعل من الفرد مجرما، وهذا ما يسمى ضمانات المحاكمة العادلة.

٣- **تحديد تقنيات الرقابة الإلكترونية وحدود استعمال المعطيات المتحصل عليها**

تكون الترتيبات التقنية الموضوعة للأغراض المراقبة الإلكترونية موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر أعلاه على غرار الأفعال الإرهابية أي الجرائم الأكثر خطورة.

أما عن التقنيات التكنولوجية التي يمكن أن تستعمل في إطار المراقبة الإلكترونية فهي تتمثل في :اعتراض المراسلات الإلكترونية[3]، تسجيل الأصوات، التقاط الصور[4]، تفتيش المنظومات المعلوماتية وحجزها(المادة 5 و7 من القانون ٠٩-٠٤، إلا أن السؤال الأهم هو ما مصير المعلومات المتحصل عليها؟

أجابت المادة 09 من القانون٠٩-٠٤ المتعلقة بحدود استعمال المعطيات المتحصل عليها عن طريق الحجز بأنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات

---

[1] نصت المادة 65 مكرر 7 من قانون الإجراءات الجزائية، على أنه : " يتضمن الإذن كل العناصر التي تسمح على التعرف على الاتصالات ويسلم مكتوبا ويكون صالحا لمدة أربعة أشهر قابلة للتجديد بنفس الشروط الشكلية والزمنية، يسلم الإذن لوضع الترتيبات بغير رضا أو علم الأشخاص الذين لهم حق على تلك الأماكن".

[2] الجريدة الرسمية العدد 53 ، الصادرة في 08 أكتوبر ٢٠١٥.

[3] تعرف المادة/ 2 والاتصالات الإلكترونية على أنها :"أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية".

[4] المادة 65 مكرر 5 من القانون رقم 19 – 15 المؤرخ في 30 ديسمبر 2015 يعدل ويتمم الأمر رقم 156 – 66 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية العدد 71 ، الصادرة في 30 ديسمبر 2015

القضائية، ما تشير إليه هذه المادة هو أن الاستعمال المشروع للبيانات الشخصية المتحصل عليها من المراقبة الإلكترونية يتحدد بحدود ضرورات التحقيقات، وهو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار.

4 -سن عقوبات لجريمة إفشاء معلومات ذات طابع شخصي ناتجة عن المراقبة الإلكترونية

يكون الموظفين القائمين على عمليات المراقبة الإلكترونية قادرين على الاطلاع على معلومات ذات طابع مجرم وأخرى ذات طابع شخصي، وفي كلتا الحالتين يكون هؤلاء مطالبين باحترام السر المهني.

لهذا جرم المشرع كل محاولة من قبل هؤلاء الموظفين نحو استغلال عمليات المراقبة لأغراض شخصية، أو كل تجاوز لحدود المراقبة الإلكترونية نحو انتهاك حرمة الحياة الشخصية للأفراد أيا كان السبب، أو إفشاء مستندات ناتجة عن التفتيش أو إطلاع عليها شخص لا صفة له قانونا في الاطلاع عليه، وذلك بغير إذن مكتوب من المتهم أو من ذوي حقوقه أو من الموقع على هذا المستند أو من المرسل إليه ما لم تدع ضرورات التحقيق إلى غير ذلك[1] .

الفرع الثاني: إجراءات تفتيش المنظومة المعلوماتية

قررت المادة٥ من القانون رقم٩ ٠٤٠، أنه يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص عليها في المادة٤ أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

-منظومة معلوماتية أو جزء منها وكذلك المعطيات المعلوماتية المخزنة فيها.

-منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة- أ- من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

وإذا تبين مسبقا بأن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

وكمثال على المساعدة القضائية الدولية كإجراء جديد لتتبع مجرمي المعلوماتية، قضية توقيف مصالح الأمن الجزائرية لشاب جزائري ببلدية بومرداس بعد تقديم المكتب الفدرالي الأمريكي للتحقيقات شكوى ضده مفاده ا أن هذا الشاب قد بعث برسالة إلكترونية لهذا المكتب مهددا فيها بوضع قنبلة في أحد أحياء مدينة جوانسبورغ بجنوب إفريقيا تستهدف المناصرين الأمريكيين قبل انطلاق المباراة الكروية بين المنتخب الجزائري والأمريكي في بطولة كأس العالم.

والمشرع الجزائري في المادة الخامسة من القانون رقم٩ ٠٤٠ نص على التفتيش المنصوص عليه في قانون الإجراءات الجزائية، وحتى وأن اختلف مضمونه عن التفتيش العادي بحيث يجب توفر شروط التفتيش المنصوص عليها في المادة 45 من قانون الإجراءات الجزائية مع مراعاة أحكام الفقرة الأخيرة منها لأننا بصدد جرائم معلوماتية.

---

[1] المادة 46 من الأمر رقم 02 – 15 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 155 – 66 المؤرخ في 8 جويلية 1966 المتضمن قانون

الإجراءات الجزائية، الجريدة الرسمية عدد 40 ، الصادرة في 23 جويلية ٢٠١٥.

غير أن القانون رقم٠٤/٠٩ أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد، وهذا إجراء جديد بحيث يمكن الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب، للتفتيش عن أدلة في المعلومات التي يحتوي عليها هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها[1].

ويمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها[2].

كما نص المشرع الجزائري، ودائما في نفس القانون 09\04 على إجراء آخر يسهل عملية التفتيش في الفقرة الأخيرة من المادة 5، وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المختصين في الإعلام الآلي وفن الحاسوبات لإجراء عمليات التفتيش على المنظومة المعلوماتية، وجمع المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات[3].

الفرع الثالث: حجز المعطيات المعلوماتية

أكدت المادة ٦ من القانون رقم٠٩\٠٤، أنه عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات، وإذا استحال إجراء الحجز وفقا لما هو منصوص عليه في أحكام المادة٠٦ أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية والى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة[4].

ويمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك[5].

وتحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية[6].

---

[1] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر 1 ، ٢٠١١-٢٠١٢، ص ١٣١-١٣٢.

[2] المادة ٠٥ من القانون رقم ٠٤/٠٩ المؤرخ في ٥ أوت ٢٠٠٩.

[3] طرشي نورة، المرجع السابق، ص ١٣٢-١٣٣.

[4] المادة ٠٧ من القانون رقم ٠٤/٠٩ المؤرخ في ٥ أوت ٢٠٠٩.

[5] المادة ٠٨ من القانون رقم ٠٤/٠٩ المؤرخ في ٥ أوت ٢٠٠٩.

[6] المادة ٠٩ من القانون رقم ٠٤/٠٩ المؤرخ في ٥ أوت ٢٠٠٩ .

وفي إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة١١ من القانون رقم٠٤٠٩ تحت تصرف السلطات المذكورة، وذلك لتمكين سلطات التحقيق من التعرف على مستعملي الخدمة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[1].

وقد حدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب من خلال المادة 12 من القانون رقم٠٤٠٩ ، على مقدمي الخدمات إلتزامات خاصة، هي:

•واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية وتقنية.

•وضع الترتيبات التقنية لحصر إمكانيات الدخول إلي الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجود[2].

المطلب الثالث: دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

وقع رئيس الجمهورية السيد عبد العزيز بوتفليقة على مرسوم رئاسي مرسوم رئاسي رقم٢٦١/١٥ المؤرخ في٢٤ من ذي الحجة عام١٤٣٦ هـ/ الموافق ل٨ أكتوبر٢٠١٥ يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تعد سلطة إدارية مستقلة لدى وزير العدل ستعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وكلفت الهيئة بتنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وتتشكل هذه الهيئة من لجنة مديرة يرأسها الوزير المكلف بالعدل وثلاثة مديريات ومركز للعمليات التقنية وملحقات جهوية، كما يتمثل أعضاؤها في الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيا

الإتصال، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا[3].

وبهذا ضمت الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية.

---

[1] المادة ١٠ من القانون رقم ٠٤/٠٩ المؤرخ في ٥ أوت ٢٠٠٩.

[2] طرشي نورة، المرجع السابق، ص ١٣٤.

[3] المادة ٦ و٧ من المرسوم الرئاسي رقم 15-261 المؤرخ في ٢٤ من ذي الحجة عام ١٤٣٦هـ/الموافق ل ٨ أكتوبر ٢٠١٥ يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها..

ويتمثل دور هذه الهيئة في تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام كالاتصالات ومكافحتها، وهي تلك التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكتَّرونية.

كما تعنى بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال وضمان مراقبة الاتصالات الالكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة، وذلك تحت سلطة القاضي المختص، وباستثناء أي هيئة وطنية أخرى.

أما فيما بخص مجال تطبيق الوقاية من هذه الجرائم ومع مراعاة الأحكام القانونية التي تضمن سرية المراسلات كالإتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيان بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية[1].

وإنشاء هذه الهيئة مكن بالفعل من تزويد العدالة بالمزيد من الموارد البشرية المؤهلة ومراجعة الترسانة التشريعية بما في ذلك في المجال الجزائي من أجل تحسين حماية حقوق وحريات المواطنين وتشديد العقوبات على أي تقصير في هذا المجال"[2].

الشكل١ : **قضايا المساس بأنظمة المعالجة الآلية للمعطيات التي طرحت على المحاكم الجزائرية**

السنة	٢٠٠٥	٢٠٠٦	٢٠٠٧	٢٠٠٨	٢٠٠٩	٢٠١٠	المجموع
عدد الجرائم	٠١	٠١	٠٣	٠٦	١٢	١٢	٣٥
عدد الأشخاص المتابعين	٠٠	٠١	٠٣	١٣	٥١	٢٠	٨٨

ولكن تثبت التقارير الإحصائية، أن هذا الرقم هو أقل بأضعاف من حجم الاعتداءات الفعلية التي أثبتت تقارير أنها تكون بين ٢٠ إلى ٢٥ اعتداء يوميا بمختلف الأشكال التي وإن وضع المشرع نظام حماية نظام المعالجة الآلية للمعطيات، إلا أنه لم تعالج نصوصه الأفعال المقترفة بشكل مفصل، والتي تتطور بشكل مذهل في الثانية الواحدة وكأنها مسابقة عالمية بين المخترقين والقراصنة حول من يبتكر أكثر جريمة انترنت تطورا وسرعة، وحتى الدول الكبرى لم تتمكن من وضع آليات ووسائل فعالة للحد من الإجرام المعلوماتي أثبتت التقارير الصادرة عن مكتب التحقيقات الفدرالي (FBI) أن جرائم الكمبيوتر تكلف الاقتصاد الأمريكي٦٧.٢ دولار سنويا، وحوالي٦٤ بالمئة من الشركات الأمريكية؛ تعرضت لخسائر مالية بسبب حوادث اختراق أنظمة الكمبيوتر خلال العام الماضي.

---

[1] برابح يمينة، "تطبيقات الأمن المعلوماتي "، بالملتقى الوطني الموسوم بـ : الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان، يومي ٧ و٨ فبراير ٢٠١٧، ص ٩.

[2] إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته التي سبق ونص عليها القانون رقم ٠٩/٠٤ المؤرخ في ٥ أغسطس ٢٠٠٩ والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أنظر: مرسوم رئاسي رقم 15-261 المؤرخ في ٢٤ من ذي الحجة عام ١٤٣٦هـ/الموافق ل ٨ أكتوبر ٢٠١٥ يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الخاتمة

في الأخير نخلص، إلى أن المشرع الجزائري لا يتوفر على آليات قادرة على الاضطلاع بالآثار الخطيرة التي ترتبها جرائم المساس بأنظمة المعالجة الآلية للمعطيات سواء على مستوى النصوص التشريعية أو على مستوى طبيعة الكوادر والأجهزة المتخصصة لمواجهة هذا النوع من الإجرام، ومن ثم كان لابد أن يبادر إلى تبني سياسة موسعة ومحكمة، تستهدف إيقاف كل التحديات التي يطرحها هذا الإجرام، وإيمانا بأهمية الوقوف أمام التحديات التي تفرضها هذه الجريمة، ارتأينا ختم هذا البحث ببعض الاقتراحات والتوصيات التي قد تساهم في التقليل من الآثار السلبية لكثير من التحديات المصاحبة لوسائل الاتصال الجديدة، وتندرج هذه التوصيات تحت النقاط الآتية:

١. إعطاء جرائم التقنية حقها من الأهمية في مؤسسات التشريع الوطنية والدولية على السواء، مع التركيز على أهمية إدراج نصوص هذه الأخيرة ضمن التشريعات الوطنية المختلفة، باعتبار أن جرائم الإنترنت ذات بعد دولي تتطلب الانخراط في اتفاقيات دولية، والاهتمام بالتعاون الدولي في مجال المكافحة لضمان الحماية العالمية الفعالة لبرامج المعطيات الآلية والكمبيوتر وشبكة الانترنت ككل.

٢. تعديل بعض التشريعات الحالية بما يتلائم مع طبيعة جرائم الإنترنت والتقنية، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات، وشرحها لهم بشكل واضح، وخاصة وأن في مجال الملكية الفكرية فالتشريع الوحيد الذي تقع برامج المعالجة الآلية للمعطيات تحت حمايته هو قانون حقوق المؤلف وحتى في هذا إطار هذا القانون لا تتعدى الحماية شكل البرنامج فقط، لهذا السبب تبرز أهمية البحث عن إطار أكبر وأوسع لبرامج الكمبيوتر يتعدى النصوص التقليدية لجريمة التقليد المنصوص عليها في قانون حقوق المؤلف والحقوق المجاورة.

٤ . نظرا لطبيعة الجريمة المعلوماتية الخاصة وكيان بيئتها غير المحسوس تظهر صعوبة مهام السلطات شبه القضائية والسلطات القضائية في أداء دورها للكشف عن الجريمة والبحث عن أدلتها فحتى؛ وإن نجحت الدّول نسبيا في تطبيق الأساليب الإجرائية التقليدية كالمعاينة والتفتيش والضبط وإضفاء بعض الخصوصيات والشروط عليها، لتتلائم وطبيعة الجريمة المعلوماتية، تبقى بعض الصعوبات دائما للكشف عن هذه الجريمة والمتمثلة في قلة الآثار المادية التي تتركها وكثرة الأشخاص الذين يترددون على مسرحها بين فترة ارتكابها وفترة اكتشافها، مما يصعب عملية الكشف عنها.

٣. عقد دورات مكثفة للعاملين في حقل التحري والتحقيق، والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوبات، والجرائم المرتبطة بها، والنظر في تضمين مناهج التحقيق الجنائي في كليات، ومعاهد تدريب الشرطة موضوعات عن جرائم الإنترنت.

٤. مساعدة شركات التقنية والإنترنت العربية في اتخاذ إجراءات أمنية مناسبة، سواء من حيث سلامة المنشآت أو ما يختص بقواعد حماية الأجهزة، والبرامج.

٥. التنسيق لإنشاء مركز معلومات عربي مشترك يهتم برصد وتحليل جرائم الحاسوب، يضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم، حيث أن جريمة الإنترنت لا تحدها حدود وطنية، أو قومية.

٦. سرعة تماشي عملية التشريع مع المعطيات الواقعية، والإسراع في إصدار القوانين التنظيمية، من خلال محاولة وضع مدونة قواعد السلوك في مجال المعلوماتية، تتناسب والتطورات التي يعرفها الإجرام المعلوماتي.

٧. كما تظهر ضرورة إيجاد الوسائل المناسبة للتعاون الدولي لمكافحة هذه الجريمة من الناحية الإجرائية بهدف التوفيق بين التشريعات الخاصة بهذه الجرائم كالتعاون الدولي على تبادل المعلومات وتسليم المجرمين وقبول أي دولة للأدلة المجموعة في دول أخرى.

٨. وأخيرا في رأينا، أن أحسن حماية هي الحماية الوقائية ن بحيث من الأفضل نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية (عدم الاحتفاظ ببيانات شخصية أو مالية على الأجهزة، عدم نشر معلومات شخصية، عدم إعطاء كلمة السر..الخ).

قائمة المراجع

أ- الكتب

١. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001.

٢. سامي صادق الملا، اعتراف المتهم، دار الفكر العربي، الطبعة الأولى، ١٩٩٨.

٣. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإ لكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، ٢٠٠٢.

٤. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، ١٩٩٩.

٥. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت، دار الجامعة الجديدة، ٢٠٠٨.

٦. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، الطبعة الثانية، ٢٠٠٧.

٧. محمد ماجد ياقوت، أصول التحقيق الإداري في المخالفات التأديبية، دراسة مقارنة، منشأة المعارف، الإسكندرية، مصر، بدون سنة نشر.

٨. محمد زكي أبو عامر، الإجراءات الجنائية، ط 8، دار الجامعة الجديدة، مصر، 2008.

٩. هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 2000.

ب- المذكرات والرسائل

طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر1، ٢٠١١-٢٠١٢.

ج- الندوات والمؤتمرات

١. برابح يمينة، تطبيقات الأمن المعلوماتي، بالملتقى الوطني الموسوم بـ : الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي ٧ و٨ فبراير ٢٠١٧.

٢. لوكال مريم، الحماية القانونية للبيانات ذات الطابع الشخصي في العالم الرقمي ، بالملتقى الوطني الموسوم بـ : الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي ٧ و٨ فبراير ٢٠١٧.

د- الاتفاقيات والقوانين

١. الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ ٢٠٠١/١١/٠٨.

٢. القانون رقم 01 - 16 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14 ، الصادرة في 07مارس 2016 .

٣. القانون رقم ١٤/٠٤ المؤرخ في ٢٠٠٤/١١/١٠ المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية العدد (٧١) لسنة ٢٠٠٤.

٤. القانون رقم ١٥/٠٤ المؤرخ في ٢٧ رمضان ١٤٢٥ هـ الموافق/لـ١٠ نوفمبر٢٠٠٤ المعدل والمتمم لقانون العقوبات رقم ١٥٦/٦٦ المؤرخ في ١٨ صفر ١٣٨٦ هـ/ الموافق ل ٨ يوليو ١٩٦٦، الجديدة الرسمية العدد (٧١) لسنة ٢٠٠٤.

٥. القانون رقم ٠٦-٢٢ مؤرخ في ٢٩ ذي القعدة عام ١٤٢٧ الموافق ٢٠ ديسمبر سنة ٢٠٠٦ والمتضمن قانون الإجراءات الجزائية، المنشور في الجريدة الرسمية رقم ٨٤ الصادرة سنة ٢٠٠٦.

٦. الأمر رقم ٠٧/٠٣ المؤرخ في ٢٠٠٣/٠٧/١٩ المتعلق ببراءات الاختراع، المعدل للأمر رقم ١٧/٩٣ المؤرخ في ١٩٩٣/١٢/٠٧ المتعلق بحماية الاختراعات المعدل للأمر ٥٤/٦٦ في ١٩٦٣/٠٣/٠٣ المتعلق بشهادات المخترعين وإجازات الاختراع.

٧. الأمر رقم ٠٥/٠٣ الصادر بتاريخ ٢٠٠٣/٠٧/١٩ المتعلق بحق المؤلف والحقوق المجاورة.

٨. مرسوم رئاسي رقم 15-261 المؤرخ في ٢٤ من ذي الحجة عام ١٤٣٦هـ/الموافق ل ٨ أكتوبر ٢٠١٥ يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53 ، الصادرة في 08 أكتوبر ٢٠١٥.

٩. القانون رقم 19 - 15 المؤرخ في 30 ديسمبر 2015 يعدل ويتمم الأمر رقم 156 - 66 المؤرخ في 8 جوان 1966 ، المتضمن قانون العقوبات، الجريدة الرسمية العدد 71 ، الصادرة في 30 ديسمبر 2015

١٠. الأمر رقم 02 - 15 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 155 - 66 المؤرخ في 8 جويلية 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 40 ، الصادرة في 23 جويلية ٢٠١٥.



الجريمة الالكترونية و آليات التصدي لها

الباحث حفوظة الأمير عبد القادر الباحث غرداين حسام مخبر الحوكمة العمومية والاقتصاد الاجتماعي جامعة أبو بكر بلقايد تلمسان.

الملخص:

إن التطور الحاصل في تكنولوجيا الإعلام والاتصال، وظهور شبكة الانترنت بكل ما حملته من تقدم وخدمات لم يمر على العالم بسلام، لأنه بقدر ما أحدث آثار ايجابية وغير نمط حياة المجتمعات وساهم في التطور والرقي في جميع المجالات ولاسيما المعاملات الالكترونية، بقدر ما كان له أثر سلبي على حياة الناس ومصالح الدول، كل هذا تجلى في تطويع الانترنت والوسائل الالكترونية لتكون عالما من عوالم الجريمة، وهكذا ظهرت إلى الوجود الجرائم الالكترونية بشتى أنواعها، وسنحاول في بحثنا هذا التطرق إلى تطور المعاملات الالكترونية ومن تم التعريف بماهية الجريمة الالكترونية وما هي الآليات الكفيلة بمكافحتها.

Abstract:

The evolution in the information and communication technology, and the emergence of the Internet with all what it carried as progress and services, this is not passed peacefully on the world, because as much as it affected positive issues and it changed in communities life style and contributed to the development and progress in all fields, particularly electronic transactions, as much as it had a negative impact on people's lives and interests of the states, all of this was reflected in the adaptation of the internet and electronic means to be a world from the worlds of crime, and so came into being the electronic crimes of various kinds, and we will try in our research that address the development of electronic transactions and the definition of what the cyber-crime and what the mechanisms to ensure combating it.

key words: Electronic transactions, cyber-crime.

مقدمة:

في ظل التطور الهائل الذي شهده مجال الإعلام والاتصال والذي رافقه التطور الكبير في تكنولوجيات الحواسيب والأجهزة الذكية، أدى ذلك إلى ظهور أدوات واختراعات وخدمات جديدة نتج عنها نوع جديد من المعاملات يسمى بالمعاملات الالكترونية والذي يقصد بها كل المعاملات التي تتم عبر أجهزة الكترونية مثل الحاسوب، شبكة الانترنيت، الهاتف المحمول(الهواتف الذكية)، و نتيجة التطور الكبير والسريع لهذه الأجهزة وضعف القدرة على المرافقة و المراقبة والتحكم، ظهر نوع جديد من الجرائم يسمى بالجريمة الالكترونية أو المعلوماتية أو التقنية ، والتي هي عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي أو الهواتف الذكية الموصولة بشبكة الانترنيت بطريقة مباشرة أو غير مباشرة لتنفيذ الفعل الإجرامي .وأصبحت هذه الجرائم في وقتنا الراهن تهدد أمن وسلامة الأفراد أو المؤسسات أو حتى الحكومات، وهو ما يقتضي الإسراع في اتخاذ الإجراءات اللازمة والتي من شأنها التقليل من حدة هذا النوع من الجرائم.

من خلال مما سبق تبرز الإشكالية الرئيسية لهذه الورقة البحثية، والمتمثلة في:

- **ما هي الجريمة الالكترونية؟ وما هي آليات التصدي لها؟**

فرضيات البحث: للإجابة على الإشكالية الرئيسية نقترح الفرضيات التالية:

- تطور المعاملات الالكترونية جعلها عرضة للجريمة الالكترونية .
- الإسراع في اتخاذ الإجراءات اللازمة لتطوير آليات التصدي للجرائم الالكترونية هو سبيل للحد منها .

أهداف البحث : تتلخص أهداف البحث فيما يلي:

- التعرف على ماهية المعاملات الالكترونية و الإطلاع على حجم التطور الذي وصلت إليه .
- التعرف على الجرائم الالكترونية التي ترافق هذه المعاملات وعلى مسببات تفشيها وعلى حجم الخسائر التي تحدثها.
- إبراز دور الحكومات في التدخل للتصدي لهذا النوع من الجرائم.

أهمية الموضوع:

ترجع أهمية موضوع الجرائم الالكترونية في الانتشار الواسع لهذا النوع من الجرائم والذي رافق الاستخدام الواسع للمعاملات الالكترونية على الصعيد الدولي والإقليمي والوطني هذا من جهة، ومن جهة أخرى فقد أصبحت الجريمة الالكترونية مُتلازمة مع التطور السريع والهائل في مجال تكنولوجيا الاتصالات والمعلومات، فنتيجة للتقدم الكبير في استخدامات الشبكة العنكبوتية(الإنترنت)، طفت الجرائم الالكترونية بصورها المُختلفة، وأصبحت تهدد الأمن المعلوماتي للأفراد، المؤسسات والحكومات.

منهج البحث المتبع :من أجل الإجابة على التساؤل المطروح وبغية اختبار الفرضيات اعتمدنا في البحث على المنهج الوصفي التحليلي والذي يتناسب مع موضوع الدراسة من خلال وصف الجرائم الالكترونية وتحليلها لتحديد أنواعها و مسبباتها ومحاولة إيجاد الآليات الكفيلة للتصدي لها.

ولتحقيق أهداف البحث، وفي ضوء الفرضيات الموضوعة، فقد تم تضمين البحث العناصر الآتية:

١- الإطار المفاهيمي للمعاملات الالكترونية:

لقد رافق التطور الهائل في تكنولوجيات المعلومات تغيير في السلوك الإداري والاقتصادي والاجتماعي، ومن بين سمات هذا التغير ظهور ما يعرف بالمعاملات الالكترونية والتي حلت محل المعاملات العادية التقليدية.

١-١- تعريف المعاملات الالكترونية:إن مصطلح المعاملات الإلكترونية يعبر عن " الانترنيت والحاسب الآلي " من حيث تبادل ونقل المعلومات والخدمات الأخرى، وكذلك مسائل تخزينها المتعلقة بالبريد، والرسائل، والسندات، والسجلات، والتواقيع والعقود الالكترونية (كعقود الخدمات، المعلوماتية، الفضائيات، الإعلانات و غيرها)، إضافة إلى التحويل الالكتروني

للأموال، إذ تعتبر جميعها من قبيل المعاملات الالكترونية[1]. والمعاملات الالكترونية بشكل عام هي انجاز الأعمال وإبرام العقود وتقديم الخدمات من خلال صيغة إلكترونية وهي تشمل كذلك جميع الأنشطة والأعمال الخاصة بتبادل البيانات والمعلومات وكذلك السلع والخدمات عبر الانترنيت (التجارة الالكترونية)، و الأنشطة المتعلقة بتنفيذ كافة الأعمال المتعلقة بالحكومة بهدف تسهيل وتسريع معاملاتها(الحكومة الالكترونية).

و يمكن تعريفها حسب ما جاء في قانون المعاملات و التجارة الالكترونية الإماراتي رقم ٠١ لسنة ٢٠٠٦: المعاملات الإلكترونية: " أي تعامل أو عقد أو اتفاقية تم إبرامها أو تنفيذها بشكل كلّي أو جزئي من خلال المراسلات الإلكترونية" [2].

وحسب ما جاء في قانون المعاملات الإلكترونية العُماني (٢٠٠٨)، فإن المعاملات الإلكترونية هي" أي إجراء أو عقد يبرم أو ينفذ كليا أو جزئي اً بواسطة رسائل إلكترونية" [3] ، ويقصد بها حسب قانون المعاملات الالكترونية السوداني (٢٠٠٧) : " العلاقات والتصرفات المالية والأحوال الشخصية وسائر المسائل القانونية غير الجنائية بما في ذلك التصرفات الفردية أو العقود التي يتم إبرامها أو تنفيذها كليًا أو جزئيًا عن طريق رسالة البيانات الالكترونية" [4].

ومن خلال ما تقدم يمكننا تعريف المعاملات الإلكترونية بأنها: " جميع المعاملات الإدارية أو التجارية أو المالية سواء أكانت حكومية أو خاصة و التي يتم تنفيذها بشكل كلي أو جزئي عن طريق الوسائط الالكترونية (حواسيب، شبكات الانترنيت، شبكات الاتصالات الهاتفية، شبكات نقل المعلومات والهواتف الذكية...الخ) بهدف تسهيل وتسريع الخدمات التجارية (التجارة الالكترونية) ، أو الخدمات الإدارية (الحكومة الالكترونية)، أو تسهيل تبادل الأموال(الصيرفة الالكترونية).

١-٢- أشكال المعاملات الالكترونية: من بين أهم أشكال المعاملات الالكترونية نجد:

١-٢-١- التجارة الالكترونية:

تعتبر التجارة الإلكترونية واحدة من التعابير الحديثة والتي أخذت بالدخول إلى حياتنا اليومية حتى أنها أصبحت تستخدم في العديد من الأنشطة الحياتية والتي هي ذات ارتباط بثورة تكنولوجيا المعلومات والاتصالات، التجارة الإلكترونية تعبير يمكن أن نقسمه إلى مقطعين، حيث أن الأول، وهو "التجارة"، والتي تشير إلى نشاط اقتصادي يتم من خلال تداول السلع والخدمات بين الحكومات والمؤسسات والأفراد وتحكمه عدة قواعد وأنظمة يمكن القول بأنه معترف بها دولياً، أما المقطع الثاني "الإلكترونية" فهو يشير إلى وصف لمجال أداء التجارة، ويقصد به أداء النشاط التجاري باستخدام الوسائط والأساليب الإلكترونية مثل الإنترنت[5].

١-١-٢-١- تعريف التجارة الالكترونية: إن التجارة بشكل عام عبارة عن مجموعة الأنشطة التي تلبي احتياجات المستهلك في المكان والزمان الملائمين، وكذلك بالسعر المناسب، أما التجارة الالكترونية (e-commerce) فهي تلك التجارة التي تتم ولكن من خلال وسيط الكتروني (الانترنيت) سواء أكان داخل حدود الدولة الجغرافية أو خارجها، وبصرف النظر عن نوعية السلع

[1] – علي خليل إسماعيل الحديثي، ماهية المعاملات الإلكترونية وتبعات التنازع القانوني فيها (دراسة مقارنة)، مجلة حولية المنتدى، المنتدى الوطني لأبحاث الفكر والثقافة – العراق، المجلد ١ العدد٧، ٢٠١١، ص ٦٥.

[2] – القانون الاتحادي رقم (1) لسنة ٢٠٠٦، المؤرخ في ٣١-٠١-٢٠٠٦، المتعلق بقانون المعاملات والتجارة الإلكترونية، الجريدة الرسمية رقم ٤٤٢، الفصل الأول، المادة ١، الفقرة ٢٦.

[3] – المرسوم السلطاني رقم (٦٩-٢٠٠٨) ، المؤرخ في ١٧-٠٥-٢٠٠٨، المتعلق بقانون المعاملات الإلكترونية، الفصل الأول، المادة ١،الفقرة ٠٤.

[4] – قانون المعاملات الالكترونية السوداني المؤرخ في ١٤-٠٦-٢٠٠٧، الفصل الأول، المادة ٢، الفقرة ١٤، ص ٤.

[5] – تجارة الكترونية، مقال منشور على موقع ويكيبيديا : https://ar.wikipedia.org/wiki/تجارة_الكترونية تاريخ الاطلاع: ٢٠١٦/٠٢/٠٧.

محل التجارة أو مدى مشروعيتها، أو القانون الذي تخضع له[1]. والتجارة الإلكترونية تعني شراء وبيع الخدمات و المنتجات من قِبل الشركات والمستهلكين من خلال الوسائط الإلكترونية المختلفة من دون استخدام أية وثائق ورقية ، وتعتبر التجارة الإلكترونية على نطاق واسع بأنها شراء و بيع المنتجات عبر الانترنت ، ولكن يمكن اعتبار بأن أية معاملة يتم الانتهاء من إجراءات بيعها بشكل كامل من خلال الإجراءات الإلكترونية يُطلق عليها تجارة إلكترونية [2]، ويعرفها قانون المعاملات والتجارة الالكترونية الإماراتي بأنها : المعاملات التجارية التي تباشر بواسطة المراسلات الإلكترونية [3]، وتعرفها منظمة التعاون الاقتصادي والتنمية (OCDE) بأنها: تشمل جميع أشكال المعاملات التجارية التي تتم بين الشركات والأفراد والتي تقوم على أساس التبادل الالكتروني للبيانات، سواء كانت مكتوبة أم مرئية أم مسموعة، هذا بالإضافة إلى شمول الآثار المترتبة على عملية تبادل البيانات والمعلومات التجارية إلكترونيا، ومدى تأثيرها على المؤسسات والعمليات التي تدعم وتحكم الأنشطة التجارية[4].

٢.١.٢.١- تقسيمات التجارة الالكترونية:

يمكن تقسيم التجارة الالكترونية حسب طبيعة العلاقات بين مختلف الأطراف الفاعلة، أو نوعية التعاملات بينهم إلى عدة أنماط[5]:

أ- التجارة الالكترونية من شركة إلى مستهلك (B2C Business to Consumer).

ب- التجارة الالكترونية من شركة إلى شركة (B2B Business to Business).

ج- التجارة الالكترونية من مستهلك إلى مستهلك (C2C Consumer to Consumer).

د- التجارة الالكترونية من مستهلك إلى شركة (C2B Consumer to Business).

هـ- التجارة الالكترونية من شركة إلى حكومة (B2G Business to Government).

و- التجارة الالكترونية بين الشركة و الموظفين (B2E :Business to Employee).

ز- التجارة الالكترونية بين الحكومة و المستهلك (G2C : Government to Consumer).

ح- التجارة الالكترونية بين الشركة و الشركاء (B2P Business to Partner).

ط- التجارة الخلوية (M- Business) .

٢.٢.١- الحكومة الالكترونية: لقد ساهمت التطورات التقنية الهائلة التي شهدها العالم مع بداية القرن الواحد والعشرين، في إحداث تغيير جذري في سير و إجراءات المعاملات الحكومية، وأصبح الانتقال من المعاملات الحكومية التقليدية إلى المعاملات الحكومية الالكترونية من أولويات الحكومات على المستوى الدولي، وذلك سعيا منها للرفع من مستوى الأداء الحكومي وتحقيق الكفاءة العالية في الأداء المؤسسي، ومواكبة التطورات التقنية التي مست جميع مناحي الحياة.

---

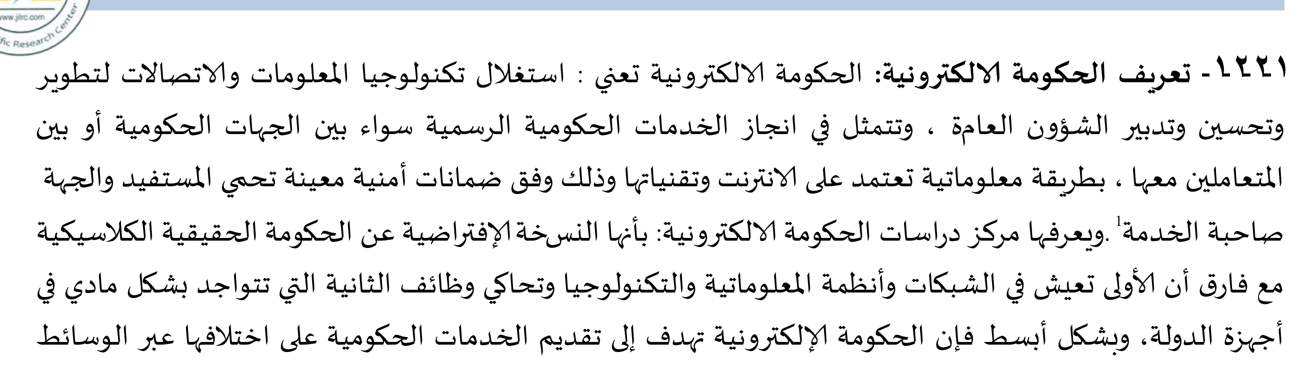
[1]- علي خليل إسماعيل الحديثي، مرجع سبق ذكره، ص٧٦.

[2]- مفهوم التجارة الالكترونية، مقال منشور على بوابة الأكاديمية العربية البريطانية للتعليم العالي على موقع : http://www.abahe.co.uk/dictionary-e-commerce.html تاريخ الاطلاع: ٢٠١٦/٠٢/٠٧.

[3]- القانون الاتحادي رقم (1) لسنة ٢٠٠٦، مرجع سبق ذكره، الفصل الأول، المادة ١، الفقرة ٢٧.

[4]- السيد أحمد عبد الخالق، التجارة الالكترونية والعولمة، منشورات المنظمة العربية للتنمية الإدارية، مصر ٢٠٠٦، ص٣٤.

[5]- أحمد بوراس، السعيد بريكة، أعمال الصيرفة الالكترونية الأدوات والمخاطر، دار الكتاب الحديث، الجزائر ٢٠١٣، ص ص ٣٦-٣٩.



١-٢-٢-١- تعريف الحكومة الالكترونية: الحكومة الالكترونية تعني : استغلال تكنولوجيا المعلومات والاتصالات لتطوير وتحسين وتدبير الشؤون العامة ، وتتمثل في انجاز الخدمات الحكومية الرسمية سواء بين الجهات الحكومية أو بين المتعاملين معها ، بطريقة معلوماتية تعتمد على الانترنت وتقنياتها وذلك وفق ضمانات أمنية معينة تحمي المستفيد والجهة صاحبة الخدمة[1] .ويعرفها مركز دراسات الحكومة الالكترونية: بأنها النسخة الإفتراضية عن الحكومة الحقيقية الكلاسيكية مع فارق أن الأولى تعيش في الشبكات وأنظمة المعلوماتية والتكنولوجيا وتحاكي وظائف الثانية التي تتواجد بشكل مادي في أجهزة الدولة، وبشكل أبسط فإن الحكومة الإلكترونية تهدف إلى تقديم الخدمات الحكومية على اختلافها عبر الوسائط الإلكترونية وأدوات التكنولوجيا وأهمها الإنترنت والاتصالات[2] .

٢-٢-٢-١- تعريف التعاملات الحكومية الالكترونية : يمكن تعريف التعاملات الحكومية الالكترونية، بأنها الاستخدام التكاملي الفعال لجميع تقنيات المعلومات والاتصالات لتنفيذ كافة الأعمال المتعلقة بالحكومة بهدف تسريع تعاملاتها سواء داخل الجهات الحكومية نفسها، أو بينها وبين تلك التي تربطها بالأفراد كمراجعين أو قطاع الأعمال[3].

٣-٢-٢-١- فوائد الحكومية الالكترونية : من بين الفوائد التي تحققها الحكومة الإلكترونية [4] :

- انجاز المعاملات الكترونيا يضمن صحة ودقة هذه المعاملات وخلوها من الأخطاء البشرية.

- توفير التكاليف المالية عند تخليص المعاملات إلكترونيا .

- ربط مختلف الوزارات ومختلف أقسام الأجهزة الحكومية يضمن إدارة أفضل وأكثر فاعلية .

- الاستفادة من الخدمات الحكومية من خلال بوابة واحدة للخدمات الالكترونية .

- الوصول إلى المعلومات التي يحتاجونها بسهولة، والتفاعل مع مختلف الأجهزة الحكومية دونما حاجة إلى الانتظار في صفوف طويلة، ودونما حاجة إلى انتظار بدء ساعات العمل أو حمل رزم ثقيلة من الأوراق .

- توفر الخدمة المناسبة للأفراد وقطاع الأعمال المناسب في الوقت المناسب.

٤-٢-٢-١- أصناف التعاملات الحكومية الالكترونية : إن للحكومة الإلكترونية أشكال متعددة تختلف باختلاف الفئة المستهدفة من أصحاب المصالح (Stakeholder) ، وتعتبر هذه الأشكال أهم القوائم التي تعتمد عليها الحكومات في إدارة أمور الدول[5]:

أ- حكومة إلى مواطن (Government to Citizen): تقوم المؤسسات الحكومية في هذا الشكل باستهداف المواطنين والمقيمين من خلال عرض ما يهمهم من معلومات مهمة وخدمات مختلفة عن طريق مواقع إلكترونية (Website) خاصة بالمؤسسة أو من خلال بوابة حكومية (Portal) مركزية، من الأمثلة على هذا النوع موقع المواطن الإلكتروني في سنغافورة (www.ecitizen.gov.sg) وموقع الحكومة المباشرة في بريطانيا (www.direct.gov.uk).

---

[1] - مريم خالص حسين، الحكومة الالكترونية، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، ٢٠١٣، ص ٤٤٣.

[2] - تعريف الحكومة الالكترونية، مركز دراسات الحكومة الالكترونية، بحث منشور على موقع http://www.egovconcepts.com/ تاريخ الاطلاع ٢٠١٧/٠٢/٠٦.

[3] - يسٌر، برنامج التعاملات الالكترونية الحكومية، مفهوم التعاملات الالكترونية، السعودية ٢٠٠٧، ص ٩.

[4] - الحكومة الالكترونية، هيئة تقنية المعلومات لسلطنة عمان، مقال منشور على موقع:
http://www.ita.gov.om/ITAPortal_AR/Info/FAQ_eGovernmen.aspx ، تاريخ الاطلاع ٢٠١٧/٠٢/٠٦.

[5] - مقال عن أشكال الحكومة الالكترونية، مدونة الدكتور حافظ الشحي ، مقال منشور بتاريخ ٢٠٠٩/١٠/٢٠ على موقع:
http://alshihi.blogspot.com/2009/10/blog-post_20.html ، تاريخ الاطلاع ٢٠١٧/٠٢/٠٦.



ب- حكومة إلى شركة (Government to Business): تقوم هنا المؤسسات الحكومية باستهداف القطاع الخاص باختلاف مؤسساته من خلال تسهيل الوصول إلى المعلومات والخدمات المهمة للشركات.

ج- حكومة إلى حكومة (Government to Government): يعتبر هذا النوع الأكثر تعقيداً من حيث استهدافه لدمج وتوحيد الخدمات والإجراءات والتعاملات الحكومية التي تتضمن أكثر من مؤسسة حكومية بمختلف تخصصاتها وبرمجياتها، ومن الأمثلة الحية على هذا النوع نجده في بوابة الولايات المتحدة الأمريكية (www.usa.gov).

د- حكومة إلى موظف (Government to Employee): لم يتم استغلال وتطوير هذا النوع كثيراً في العالم، حيث تهدف تطبيقات هذا الجانب إلى قيام المؤسسات الحكومية بإدارة معاملاتها واتصالاتها بموظفيها باستخدام تقنية المعلومات.

هـ- الحكومة الإلكترونية بإستخدام الهاتف المحمول (Mobile Government): يعتبر هذا النوع الأحدث من بين الأشكال السابقة حيث بدأ مع تطور تقنيات الاتصالات والشبكات اللاسلكية، يمكن أن نجد هذا النوع في جميع الأنواع المذكورة السابقة ويتميز بتوظيفه للأجهزة المحمولة كالهاتف النقّال وأجهزة الحاسوب المحمولة للوصول للأفراد بطريقة سريعة وسهلة وأكثر تلاؤما لأنماط حياة الناس المختلفة.

١-٢-٣- الصيرفة الالكترونية: في ظل التطور التكنولوجي الحاصل ومن اجل القدرة على المنافسة، أصبح من الواجب على البنوك أن تعدل من استراتيجياتها لخدمة زبائنها بشكل أفضل، وذلك من خلال تطوير أنظمة معلوماتها لتنتقل من التعامل التقليدي الى التعامل الالكتروني وذلك حتى توفر لزبائنها خدمة أكثر سهولة وبأقل تكلفة عن طريق استخدام وسائط الكترونية.

١-٢-٣-١-تعريف الصيرفة الالكترونية: هناك عدة تعاريف للصيرفة الالكترونية نذكر منها:

يعرفها **سفر أحمد** على أنها صناعة مصرفية جديدة تركز فيها المصارف على تقديم خدماتها عبر وسائل الكترونية، سواء في المنزل(home banking)، أو في المكتب(office banking)، أو بواسطة الهاتف الثابت(phone banking)، أو الهاتف الجوال(mobile banking) أو الانترنيت (internet banking)، وغيرها من الركائز الالكترونية المتطورة المعروفة في عالم تكنولوجيا المعلومات والاتصالات[1] ، ويقصد بالصيرفة الالكترونية الإيصال الآلي للخدمات والمنتجات المصرفية (التقليدية والحديثة) مباشرة إلى العملاء من خلال قنوات الاتصال التفاعلية الالكترونية، وهي تشتمل على الأنظمة التي تمكن عملاء المؤسسات المالية (المصارف)، سواء الأفراد أو الشركات من الوصول إلى حساباتهم المصرفية، وتنفيذ المعاملات التجارية أو الحصول على المعلومات المتعلقة بالخدمات والمنتجات المصرفية من خلال شبكة عامة أو خاصة ومن ضمنها شبكة الانترنيت، ويمكن للعملاء أن يصلوا إلى الخدمات المصرفية الالكترونية باستخدام جهاز الكتروني ذكي مثل أجهزة الكمبيوتر الشخصية (PC) أو المساعد الرقمي الشخصي (PDA) أو ماكنة الصراف الآلي (ATM) ...الخ[2].

ويعرف **سّروع جو** العمل المصرفي الالكتوني بأنه " يضم كافة العمليات أو النشاطات التي يتم عقدها أو تنفيذها أو الترويج لها بواسطة الوسائل الالكترونية أو الضوئية مثل : الهاتف والحاسوب والصراف الآلي والانترنيت والتلفزيون الرقمي وغيرها، وذلك من قبل المصارف والمؤسسات المالية، وكذلك العمليات التي يجريها مصدرو البطاقات الالكترونية، وكافة

[1] - أحمد سفر، العمل المصرفي الالكتروني في البلدان العربية، المؤسسة الحديثة للكتاب، طرابلس، لبنان، ٢٠٠٦، ص ٦٣.

[2] - FFIEC, Federal Financial Institutions Examination Council, B-Banking, IT Examination Handbook, August 2003, p1.

المؤسسات التي تتعامل بالتحويلات النقدية إلكترونياً[1] ، فيما يرى البعض الآخر الصيرفة الالكترونية بأنها " تلك البنوك والمؤسسات المالية التي أصبحت تنفذ أعمالها آليا، من خلال توظيف تكنولوجيات المعلومات والاتصالات لتقديم كافة الخدمات بالسرعة والدقة اللازمين وبأقل تكلفة وأقل جهد في ظل تحقق الأمان، والخدمات المصرفية الالكترونية تعني العملية التي من خلالها يؤدي العملاء المعاملات المصرفية الكترونيا من دون زيارة المؤسسة "[2].

٢-٣-٢-١-أنماط الصيرف الالكترونية: تتنوع أنماط الصيرفة الالكترونية لتشمل الخدمات الآتية[3]:

أ- الصيرفة الالكترونية من خلال الحاسوب الشخصي (PC Banking): تعد من أشكال الخدمات المصرفية عبر الانترنيت والتي تمكن العميل من تنفيذ المعاملات المصرفية عن طريق حاسوب شخصي مزود ببرنامج محاسبي ومالي يتيح له إجراء معاملاته المالية في منزله .

ب- الصيرفة عبر الهاتف المصرفي:تعتمد هذه الخدمة على وجود ترابط بين فروع المصرف الواحد، حيث يقوم العميل بالاتصال برقم موحد للحصول على خدمة محددة من مصرفه، أين يجد موظفا خاصا يقوم بالرد عليه للوصول إلى بياناته ومن تم تقديم الخدمة له.

ج- الصيرفة عبر الهاتف النقال: تشمل الخدمات المصرفية عبر الهاتف النقال الخدمات المعلوماتية، كالاستعلام عن الأرصدة والاطلاع على عروض المصارف و استعار العملات، وتشتمل أيضا على الخدمات المالية كتحويل الأرصدة من حساب إلى آخر وخدمات الدفع النقدي وفتح حسابات وغلقها، وغيرها من الخدمات المصرفية.

د- بنوك الانترنيت(Internet Banking): تختلف بنوك الانترنيت عن بنوك الحاسوب الشخصي في أنها لا تحتاج إلى حزمة برمجية خاصة بها تكون مثبتة على جهاز معين، وإنما من خلال الموقع الالكتروني للبنك بحيث يتم توفير قناة يتم من خلالها إجراء العمليات المصرفية ككشف الحساب أو تسديد الفواتير أو شراء شيء معين.

هـ- الصرافات الآلية (ATM): يعتبر الصراف الآلي من أهم أنماط الصيرفة الالكترونية حيث يتيح للزبائن خدمة سحب الأموال ومراقبة الأرصدة طوال اليوم ، إذ يقوم بربط الزبون بقاعدة بيانات المصرف ، ويتيح له القدرة على سحب أمواله المودعة وذلك عن طريق بطاقة خاصة يتم إدخالها في الصراف الآلي .

١-٣- أمن المعاملات الالكترونية: رغم ما تمتاز به المعاملات الالكترونية عن غيرها من الوسائل التقليدية، سواء من خلال التقنية العالية التي تمتاز بها أو السرعة في الانجاز، وصولا إلى خفض تكاليف إجراء المعاملات، إلا أنها تبقى عرضة للعديد من المشاكل والتحديات لعل أهمها هو وجود بعض الثغرات الأمنية، و التي يمكن أن تسهل عملية اختراق المواقع الالكترونية وأنظمة المعلومات وسرقة البيانات والمعلومات الموجودة بها والتي غالبا ما تتم من قبل مجاميع متخصصة في القرصنة والسرقة الالكترونية (مثل الهاكرز) وغيرهم من قراصنة الانترنيت وذلك باستخدام تقنيات خاصة بالاختراقات المعلوماتية[4]، هذه الممارسات أصبحت فيما بعد تعرف بالجريمة الالكترونية، أو الجريمة المعلوماتية (Cybercrime)، وهذا النوع من الجرائم أصبح يشكل تهديدا كبيرا لهذه المعاملات، وذلك لأن غياب السرية والأمان في تداول المعلومات، سيضعف عامل

[1] - سروع جو، العمل الالكتروني في المصارف بين الضروريات والمحاذير، اتحاد المصارف العربية، جمعية اتحاد المصارف العربية، المجلد ٢٠، العدد ٢٣٨، بيروت، اكتوبر ٢٠٠٠، ص ١٠٩.

[2] - أحمد بوراس، السعيد بريكة، مرجع سبق ذكره، ص ص ١٠٠، ١٠١.

[3] - أحمد بوراس، السعيد بريكة، مرجع سبق ذكره، ص ١٠٢-١٠٧.

[4] - علي خليل إسماعيل الحديثي، مرجع سبق ذكره، ص ٦٨.

الثقة لدى الأفراد في تبادل بياناتهم في ظل التخوف من ضياعها أو تسربها[1]، وهذا التحدي يتطلب من الجهات الرسمية، وضع قوانين وأنظمة حماية تضمن سرية المعلومات وأمانها.

٢- ماهية الجرائم الالكترونية.

٢-١-مفهوم الجريمة الإلكترونية : الجريمة الالكترونية عدة مسميات فمنهم من ينعتها بجرائم الحاسوب أو الانترنيت، أو جرائم التقنية العالية أو جرائم الياقات البيضاء، ومع تعدد المسميات تتعدد التعاريف فمنهم من يعرفها من جانب فني (تقني)، أما التعاريف الأخرى فيطغى عليها الجانب القانوني.

فمنهم من يعرف الجريمة المعلوماتية على أنها فعل ضار يستخدم الفاعل، الذي يفترض أن لديه معرفة بتقنية الحاسوب، نظاماً حاسوبياً أو شبكةً حاسوبيةً للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها أو جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة[2]، ويعرفها **أحمد صياني** بأنها تصرف غير مشروع يؤثر في الأجهزة و المعلومات الموجودة عليها وهذا التعريف يعتبر جامع مانع من الناحية الفنية للجريمة الالكترونية حيث انه لارتكاب الجريمة يتطلب وجود أجهزة كمبيوتر زيادة على ربطها بشبكة معلوماتية ضخمة[3] ، ويعرفها آخرون على أنها جريمة ذات طابع مادي , تتمثل في كل فعل أو سلوك غير مشروع، من خلال استعمال الوسائط الإلكترونية , حيث تتسبب في تحميل أو إمكانية تحميل المجني عليه خسارة , وحصول أو إمكانية حصول مرتكبه على أي مكسب، وتهدف هذه الجرائم إلى الوصول غير المشروع لبيانات سرية غير مسموح بالاطلاع عليها ونقلها ونسخها أو حذفها , أو تهديد وابتزاز الأشخاص والجهات المعنية بتلك المعلومات، أو تدمير بيانات وحواسيب الغير بواسطة فيروسات[4] .

والبعض الآخر يعرفها بأنها"الجرائم التي ترتكب ضد أفراد أو مجموعات مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية، أو التسبب بالأذى الجسدي أو النفسي للضحية بشكل مباشر أو غير مباشر، باستخدام شبكات الاتصال الحديثة مثل الإنترنت (غرف الدردشة، البريد الإلكتروني..)، والهواتف الجوالة (الرسائل النصية القصيرة ورسائل الوسائط المتعددة)، وتشمل الجرائم الإلكترونية أي فعل إجرامي يتم من خلال الحواسيب أو الشبكات كعمليات الاختراق والقرصنة، كما تضم أيضا أشكال الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت[5]، ولقد عرفها الدكتور عبد الفتاح مراد على أنها :" جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت وهي تتطلب إلمام خاص بتقنيات الحاسب الآلي و نظم المعلومات سواء لارتكابها أو للتحقيق فيها ويقصد بها أيضا أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الانترنت مثل مواقع الانترنت وغرف المحادثة أو البريد الالكتروني كما تسمى كذلك في هذا الإطار بالجرائم السيبيرية أو السيبرانية لتعلقها بالعالم الافتراضي"، وهناك من يسميها أيضا بجرائم التقنية العالية

[1]- يسٌر، برنامج التعاملات الالكترونية الحكومية، مرجع سبق ذكره، ص ١٥.

[2]- كامل فريد السالك، الجريمة الالكترونية، محاضرة ألقيت في ندوة التنمية ومجتمع المعلوماتية ٢١-٢٣ أكتوبر ٢٠٠٠، الجمعية السورية للمعلوماتية، حلب، سورية.

[3]- إسراء جبريل رشاد مرعي، الجرائم الالكترونية- الأهداف-الأسباب-طرق الجرائم ومعالجتها، مقال منشور على الموقع الالكتروني للمركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، قسم الدراسات المتخصصة، على الرابط : http://democraticac.de/?p=35426 تاريخ الاطلاع ٢٠١٧/٠٢/١٣.

[4]- منى شاكر فراج العسبلي، تأثير الجريمة الالكترونية على النواحي الاقتصادية، مقال منشور على موقع كنانة أونلاين على الرابط : http://kenanaonline.com/users/ahmedkordy/posts/320920 تاريخ الاطلاع:٢٠١٧/٠٢/١٣.

[5]- رماح الدلقموني، الجرائم الالكترونية.. عندما تصبح التقنية وسيلة للإجرام، مقال منشور على موقع الجزيرة الإخبارية الالكتروني، قسم علوم وتكنولوجيا، بتاريخ ٢٠١٥/٠٤/٠٦ على الرابط: http://www.aljazeera.net/news/scienceandtechnology/2015/4/6 تاريخ الاطلاع ٢٠١٧/٠٢/١٣.

أو جرائم أصحاب الياقات البيضاء[1]. وعرفتها منظمة التعاون الاقتصادي والتنمية (OCDE) بأنها: كل سلوك غير مشروع، أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها[2].

و قد اصطلح المشرع الجزائري على تسمية الجرائم الالكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وعرفها بموجب المادة٢ من القانون٠٩-٠٤ المؤرخ في٠٥ غشت٢٠٠٩، على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية[3].

٢-٢ **خصائص الجريمة الإلكترونية** :تتميز الجريمة الإلكترونية بخصائص وصفات تميزها عن غيرها من الجرائم الأخرى ومن بين أهم هذه الخصائص ما يلي[4]:

١ - مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها ، في حين أن مرتكب الجريمة التقليدية في – الغالب - شخص أمي بسيط ، متوسط التعليم .

٢- مرتكب الجريمة الإلكترونية – في الغالب – يكون متكيفا اجتماعيا وقادرا ماديا ، باعثه من ارتكاب جريمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي، في حين أن مرتكب الجريمة التقليدية – غالبا – ما يكون غير متكيف اجتماعيا وباعثه من ارتكابه الجريمة هو النفع المادي السريع.

٣- تقع الجريمة الإلكترونية في مجال المعالجة الآلية للمعلومات وتستهدف المعنويات لا الماديات .

٤- الجريمة الإلكترونية ذات بعد دولي ، أي أنها عابرة للحدود ، فهي قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية ، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.

٥- هي جريمة ناعمة، تنفذ بسرعة وهي صعبة الإثبات:ناعمة أي أنها لا تتطلب لارتكابها العنف ولا استعمال الأدوات الخطيرة كالأسلحة وغيرها، فنقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلا لا تحتاج إلا إلى لمسات أزرار، تنفذ بسرعة أي أنها تتميز بإمكانية تنفيذها بسرعة فأغلب الجرائم المعلوماتية ترتكب في وقت قصير جداً قد لا يتجاوز الثانية الواحدة، وفي المقابل فهي صعبة الإثبات لعدم وجود الآثار المادية التقليدية (مثل بقع الدم، تكسير، خلع...الخ .)وهذا ما جعل وسائل الإثبات التقليدية غير كافية، مما أدى إلى البحث عن أدلة فعالة لإثباتها، كاستخراج البصمات الصوتية أو استعمال شبكية العين ومضاهاتها باستخدام وسائل آلية سريعة[5].

---

[1] – إسراء جبريل رشاد مرعي، مرجع سبق ذكره.

[2] – يونس عرب، صور الجرائم الالكترونية واتجاهات تبويبها، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، مسقط، سلطنة عمان،٢-٤ ابريل ٢٠٠٦، ص ٧.

[3] – القانون رقم ٠٩-٠٤ المؤرخ في ٠٥ غشت ٢٠٠٩، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم ٤٧، ص ٥.

[4] – مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بالسودان المنعقد في ٢٣-٢٠١٢/٩/٢٥، ص ١٦.

[5] – كامل فريد السالك، مرجع سبق ذكره.

٦- الجاذبية: نظرا لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الأجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويلا مسارها أو استخدام أرقام البطاقات...الخ[1].

٧- امتناع المجني عليهم عن التبليغ: لا يتم في غالب الأحيان الإبلاغ عن جرائم الانترنيت إما لعدم اكتشاف الضحية لها و إما خشية من التشهير، لذا نجد أن معظم جرائم الانترنيت تم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها[2].

٨- سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول إليه: يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتم عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسوب على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما إن يحس الجاني بأن أمره سينكشف حتى يبادر بإلغاء هذه الأوامر، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبيها،أمر في غاية الصعوبة[3].

٣-٢- أصناف الجرائم الإلكترونية: لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم الالكترونية وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو دافع المجرم، أو على أساس محل الجريمة، و على هذا الأساس يمكن تقسيمها إلى[4]:

١-٣-٢- الجرائم الواقعة على الأموال: في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الالكترونية، وما انجر عنه من تطور في وسائل الدفع والوفاء، وفي خضم التداول المالي عبر الانترنيت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم ومنها:

- السطو على أرقام بطاقات الائتمان والتحويل الالكتروني الغير مشروع.
- القمار وغسيل الأموال عبر الانترنيت.
- ج- جريمة السرقة والسطو على أموال البنوك.
- د- تجارة المخدرات عبر الانترنيت.

٢-٣-٢- الجرائم الواقعة على الأشخاص:

مع تطور شبكة الانترنيت أصبحت المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، مما جعلها عرضة للانتهاك والاستعمال من طرف هؤلاء المجرمين وجعلت سمعة وشرف الأفراد مستباحة، ومن أهم هذه الجرائم ما يلي:

- جريمة التهديد والمضايقة والملاحقة.
- انتحال الشخصية والتغرير و الاستدراج.
- ج- صناعة ونشر الإباحة.

---

[1] – عبد العال الديربي، الجريمة المعلوماتية.تعريفها..أسبابها..خصائصها،دوريات مفاهيم إستراتيجية، المركز العربي لأبحاث الفضاء الالكتروني، مقال منشور بتاريخ ٢٠١٣/٠١/١٣ على الرابط: http://accronline.com/article_detail.aspx?id=7509 تاريخ الاطلاع ٢٠١٧/٠٢/١٣.

[2] – محمد صالح العادلي، الجرائم المعلوماتية (ماهيتها وصورها)، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، سلطنة عمان،٢-٤ أفريل ٢٠٠٦، ص ٧.

[3] – موسى مسعود أرحومة، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتية عبر الوطن، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ٢٠٠٩، ص٣.

[4] – صغير يوسف، الجريمة المرتكبة عبر الانترنيت، رسالة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، ٢٠١٣، ص ٤٣-٥٨.



- د- جرائم القذف والسب وتشويه السمعة.

٢-٣-٣- الجرائم الواقعة على أمن الدولة: من أهم الجرائم الالكترونية التي تهدد أمن الدول ومجتمعاتها ما يلي:

أ- الجماعات الإرهابية: استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للانترنيت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها.

ب- الجريمة المنظمة: استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الاتصال والانترنيت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ العمليات الإجرامية بيسر وسهولة[1].

ج- الجرائم الماسة بالأمن الفكري:يبقى الأمن الفكري من بين أخطر الجرائم المرتكبة عبر الانترنيت، حيث تعطي الانترنيت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة للهزيمة الفكرية وهو ما يسهل خلق الفوضى.

د- جريمة التجسس الالكتروني: سهلت شبكة الانترنيت الأعمال التجسسية بشكل كبير حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلوماتية ثلاث أهداف رئيسية وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي[2].

٢-٤- واقع الجريمة الالكترونية:

٢-٤-١- الجريمة الالكترونية حقائق وأرقام: مع شيوع استخدام الكمبيوتر أواخر سبعينات القرن الماضي برزت ظاهرة القرصنة الإلكترونية، وسرعان ما تحول السلوك الذي بدا في بدايته انحرافا لمراهقين شغوفين بالتكنولوجيا، حربا تشن بين الدول، وهي تهدد منشئات حيوية كالمفاعلات النووية ومحطات الكهرباء كما تدمر المخزونات النقدية لبنوك ودول وتهتك أسرارا لا يراد لها الخروج إلى العلن[3]، وكشفت أرقام وبيانات عالمية، تزايد الجرائم الالكترونية في مختلف أنحاء العالم، مع التوسع المتزايد لاستخدام الانترنت والأجهزة الذكية، وأظهرت دراسة لموقع "أرقام ديجتال" أن عدد ضحايا الهجمات والجرائم الالكترونية، يبلغ ٥٥٦ مليون مستخدم سنويا، وأكثر من ١.٥ مليون ضحية يوميا، في حين تقع ضحية كل ثانية لهذه الهجمات، وأكثر أنواع الجرائم سرقة هويات وعددها ٢٢٤ مليون سرقة، وأظهرت الدراسة أن مواقع التواصل الاجتماعي هي الأكثر اختراقا، إذ بينت أن أكثر من ٦٠٠ ألف حساب فيسبوك يتم اختراقها يوميا وبينت الدراسة أن الكلفة السنوية المخصصة للأمن المعلوماتي قدرت بـ ١٠٠ مليار دولار، بعدما كانت في حدود ٦٣,٧ مليار دولار سنة ٢٠١١، ومن المتوقع أن تتجاوز ١٢٠ مليار دولار بحلول سنة ٢٠١٧[4]، وحسب تقرير نشرته شركة مشاريع الأمن السيبراني(CYBERSECURITY VENTURES) بعنوان: Cyber Security Economy predictions 2017-2021، فإن العالم سينفق ما قيمته ١ تريليون دولار خلال الفترة التي تمتد من ٢٠١٧ الى غاية ٢٠٢١ على منتجات وخدمات الأمن السيبراني لمكافحة الجريمة الالكترونية و في هذا الإطار

---

[1] – سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنيت، دار الفكر الجامعي، الإسكندرية ٢٠٠٧، ص ٨٣.

[2] – علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، الطبعة الأولى ٢٠١١، ص ٩٦-٩٧.

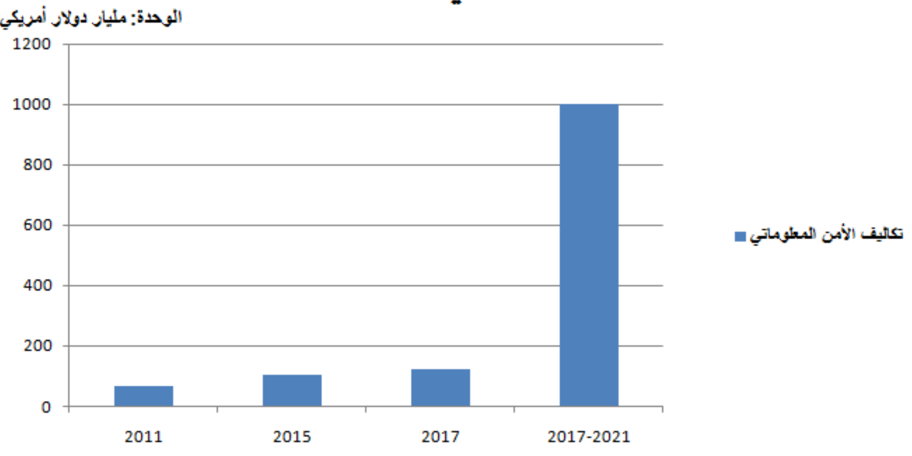
[3] – القرصنة الالكترونية سلاح العصر الرقمي، مقال منشور على موقع قناة الجزيرة الالكتروني بتاريخ :٢٠١٥/٠١/٠٥، http://www.aljazeera.net/knowledgegate/newscoverage/2015/1/5/القرصنة_الالكترونية_سلاح_العصر_الرقمي ، تاريخ الاطلاع ٢٠١٧/٠٢/١٠.

[4] – احصائيات صادمة وغريبة عن جرائم الأمن المعلوماتي، دراسة مقدمة من طرف موقع أرقام ديجيتال بتاريخ ٢٠١٥/١٠/٢٥ متوفرة على موقع : http://digital.argaam.com/article/detail/112326 ، تاريخ الاطلاع : ٢٠١٧/٠٢/١١.

فقد سجل فتح حوالي مليون وظيفة خاصة بالأمن السيبراني خلال سنة ٢٠١٦، ومن المتوقع أن يكون هناك عجز بحوالي ١,٥ مليون وظيفة خلال عام ٢٠١٩[1].

والشكل الموالي يوضح تطور تكاليف الأمن السيبراني أو المعلوماتي خلال الفترة الممتدة من ٢٠١١ والى غاية ٢٠٢١.

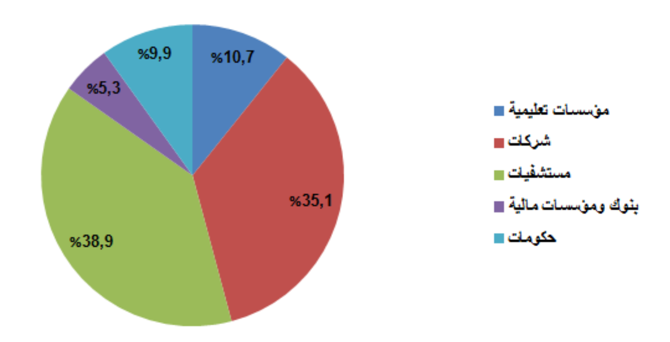
الشكل رقم 1: تكاليف الأمن المعلوماتي خلال الفترة من 2011 الى 2021



المصدر: من إعداد الباحثين اعتمادا على معطيات موقع أرقام ديجيتال و cybersecurity ventures .

والشكل الموالي يبين أكثر المؤسسات أو الشركات تعرضا للاختراق خلال سنة ٢٠١٥.

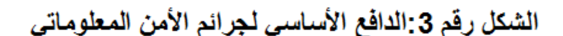
الشكل رقم 2:اكثر الشركات والمؤسسات اختراقا خلال 2015

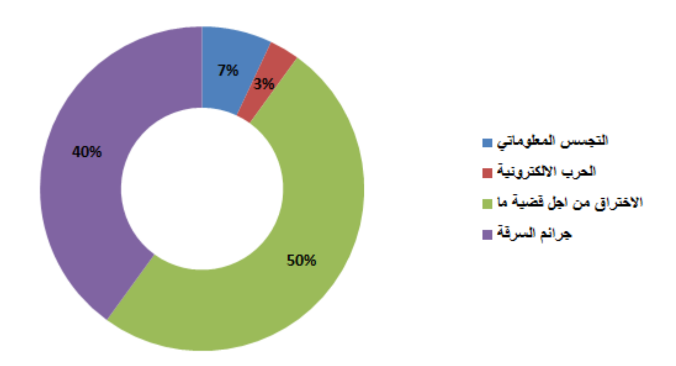


المصدر: من اعداد الباحثين اعتمادا على دراسة لموقع ارقام ديجيتال على الموقع التالي:
http://digital.argaam.com/article/detail/112326

أما بالنسبة للدوافع الأساسية للإجرام المعلوماتي فقد تباينت ما بين جرائم من اجل السرقة، بدافع التجسس المعلوماتي، الحرب الالكترونية أو الاختراق من أجل قضية ما، والشكل الموالي يوضح النسب المئوية المقابلة لذلك.

[1] - cyber security economy predictions 2017-2021,cybersecurity ventures 2016 .


الشكل رقم 3:الدافع الأساسي لجرائم الأمن المعلوماتي

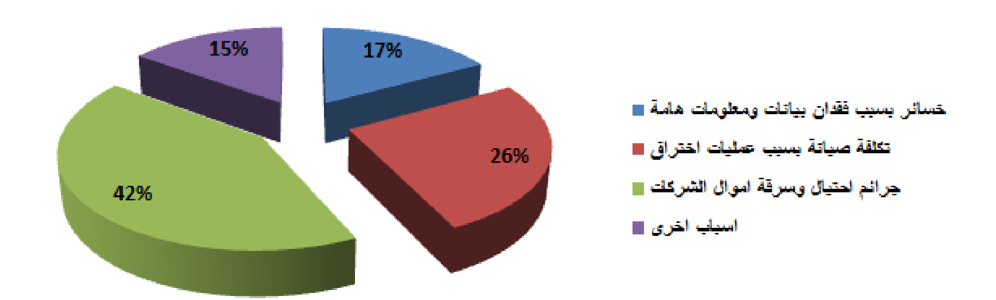


المصدر :من اعداد الباحثين اعتمادا على دراسة لموقع ارقام ديجيتال على الموقع التالي:

http://digital.argaam.com/article/detail/112326

ومن المتوقع أن تكبد الجرائم الالكترونية الاقتصاد العالمي حوالي ٦ تريليون دولار بحلول سنة ٢٠٢١ وهي ضعف الخسائر المسجلة سنة ٢٠١٥ والمقدرة بحوالي ٣ تريليون دولار[1] ، وأكثر الخسائر تحدث إما بسبب فقدان بيانات ومعلومات هامة أو نتيجة لتكلفة صيانة عمليات الاختراق أو بسبب احتيال وسرقة أموال من الشركات، والشكل الموالي يوضح ذلك :

الشكل رقم 4:اسباب خسائر الجرائم الالكترونية



المصدر :من اعداد الباحثين اعتمادا على دراسة لموقع ارقام ديجيتال على الموقع التالي:

http://digital.argaam.com/article/detail/112326

ولقد عايشنا خلال سنتي ٢٠١٥و٢٠١٦ العديد من حوادث الاختراق والقرصنة ولعل أهمها مايلي:

١- في سبتمبر من سنة ٢٠١٦، كشفت شركة ياهوو(yahoo) عن أكبر عمليات قرصنة وسرقة لقاعدة بيانات مستخدميها، هذه العملية تُعتبر من أكبر عمليات القرصنة في التاريخ لشركة تقنية، حيث حصل القراصنة على بيانات أكثر ٥٠٠ مليون مستخدم ، و في ديسمبر من نفس السنة تعرضت الشركة نفسها، لصدمة أخرى حيث أعلنت بأن بيانات أكثر من مليار

[1] - cyber security economy predictions 2017-2021, Op. Cit.

مستخدم قد تم الاستيلاء عليها وأصبحت معروضة للبيع ، منها كلمات السر وأسئلة الأمان وأرقام هواتف وتواريخ ميلاد، هذه الحوادث خفضت من أسهم الشركة الأمريكية اقتصاديا وإعلامياً بشكل ملحوظ[1].

٢- لقد واجه مستخدمو الإنترنت حول العالم يوم٢١/١٠/٢٠١٦، صعوبات في دخول المواقع الالكترونية الرئيسية، وهذه المشكلة تسببت في سقوط أهم مواقع العالم، مع تردد أنباء عن أن سبب المشكلة هجمات إلكترونية، وبحسب موقع Business Insider، فقد تعرضت أهم مواقع العالم لهجوم الحرمان من الخدمة (DDOS) والذي يعتبر أكثر الهجمات الإلكترونية شيوعاً في عالم الإنترنت و الذي يستهدف DNS ، وهي أهم فقرة في منظومة الانترنت، إذ تعمل على ترجمة عنوان الموقع إلى عنوان IP، وأبرز المواقع الرئيسية التي تعرضت للسقوط هي Amazon ، Twitter، Github Etsy, Spotify[2].

٣- كشف محققون عما يعتقدون أنه أكبر جريمة إلكترونية في التاريخ، سرق خلالها قراصنة روس من العديد من بنوك دول العالم (شملت مصارف في اليابان والصين والولايات المتحدة، مروراً بمصارف في الدول الأوروبية)، ما يصل إلى مليار دولار، وهي العملية التي وصفت بأنها "ثورة في عالم الجريمة الإلكترونية" ، وهذه السرقة تشكل علامة فارقة على بداية مرحلة جديدة في ثورة النشاط الإجرامي الإلكتروني، حيث يسرق المستخدمون الأموال مباشرة من البنوك ويتجنبون المستخدمين العاديين[3].

٢-٤- واقع الجريمة الالكترونية في الوطن العربي:

لقد أصبحت الهجمات الإلكترونية مصدر تهديد حقيقيا لاقتصاديات الدول، ولم تعد هذه الجرائم تقتصر على سرقة أموال البنوك أو الأفراد، بل اجتاحت قطاعات جديدة على غرار أمن الموانئ، التي قد تتعرض لهجمات خطيرة من عصابات الجريمة المنظمة أو الإرهابيين أو حتى الدول المعادية، وذكر بعض الخبراء أن الأرباح الضخمة التي تحققها الجرائم الإلكترونية تجاوزت أرباح تجارة المخدرات، وذكر الخبراء أيضا أن الجرائم الإلكترونية أصبحت اليوم واقعاً في دولة الإمارات، بوقوع نحو مليوني شخص من سكان الدولة ضحية للجرائم الإلكترونية خلال سنة ٢٠١٥[4].

وكشف موقع «جوبال ريسك إنسايتس» أن المملكة العربية السعودية هي البلد الأكثر استهدافا بالهجمات الإلكترونية في الشرق الأوسط، وأن إيران أكثر من يستهدفها إلكترونيا، ونوه التقرير إلى أن الهجمات الإلكترونية على المملكة وصلت عام ٢٠١٥ إلى ١٦٠ ألف محاولة هجوم يوميا، ويشير نفس التقرير إلى أن الإمكانيات الرقمية والالكترونية الكبيرة للسعودية تجعلها هدفا مميزا للهجمات الالكترونية حيث تمتلك المملكة أكبر عدد من المشتركين في خدمة الإنترنت في العالم العربي[5]. و حسب تقارير دولية مستقلة، فإن الإمارات سجلت أفضل أداء في صد الهجمات الإلكترونية في منطقة الشرق

---

[1]- مدثر النور أحمد، أكبر حوادث الاختراق حجمًا وتأثيرًا في العالم للعام ٢٠١٦!، مقال منشور:٢٠١٦/١٢/٢٥، على موقع: http://www.arageek.com/tech/2016/12/25/2016-hacking-operations.html ، تاريخ الاطلاع ٢٠١٧/٠٢/١١

[2]- الانترنيت ينهار.. والطائر الأزرق يكف عن التغريد، مقال منشور بتاريخ ٢٠١٦/١٠/٢٢، على موقع:http://bab.com/Node/275623 تاريخ الاطلاع: ٢٠١٧/٠٢/١١.

[3]- أكبر سرقة بالتاريخ.. متسللون سرقوا مليار دولار، مقال منشور على موقع« عربية SKY NEWS »، بتاريخ ٢٠١٥/٠٢/١٦ على الرابط: http://www.skynewsarabia.com/web/article/724420 تاريخ الاطلاع: ٢٠١٧/٠٢/١١.

[4]- الجرائم الإلكترونية.. أرباح تفوق ما تجنيه تجارة المخدرات، مقال منشور على الموقع الالكتروني لجريدة الاتحاد بتاريخ :٢٠١٦/٠٢/٠٥، http://www.alittihad.ae/details.php?id=5035&y=2016&article=full ، تاريخ الاطلاع ٢٠١٧/٠٢/١٠.

[5]- محمد خالد، السعودية الأكثر تعرضا للهجمات الإلكترونية في الشرق الأوسط، مقال منشور على موقع الخليج الجديد بتاريخ :٢٠١٦/٠٨/٠١، http://thenewkhalij.org/ar/node/43159 ، تاريخ الاطلاع ٢٠١٧/٠٢/١١.

الأوسط خلال النصف الأول من سنة٢٠١، في الوقت الذي أكدت هيئة تنظيم الاتصالات على فعالية منظومة الحماية الإلكترونية في الدولة[1].

و منذ عام٢٠١، ارتفعت معدلات ما يُطلق عليه قانوناً اسم الجريمة الإلكترونية في لبنان، ما وضع المعنيين في المصارف والمؤسسات المالية والأجهزة الأمنية أمام سباق مع القراصنة القادرين على تطوير أدواتهم وتكتيكاتهم بموازاة تطور وسائل المكافحة، حيث بلغ عدد عمليات القرصنة الإلكترونية التي تعرضت لها المصارف اللبنانية حصراً منذ عام٢٠١ حتى الفصل الثالث من سنة٢٠١، وفق أرقام هيئة التحقيق الخاصة لدى مصرف لبنان٢٣٣ عملية، وصلت فيها قيمة الأموال التي تعرضت للقرصنة إلى نحو٢٦ مليوناً ونصف مليون دولار، من ضمنها١٥ مليون دولار بين عامي٢٠١٥و٢٠١٦ طالت القطاع المصرفي بشكل مباشر، وفق رئيسة مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية، المقدم سوزان الحاج. وتعكس هذه الأرقام الحد الأدنى، إذ إن القيمة الفعلية للغنائم وعدد العمليات الإلكترونية، باعتراف هيئة التحقيق ومكتب مكافحة الجرائم المعلوماتية، أكبر بالتأكيد، لأن هناك حالات لم يتم الإبلاغ عنها إما بدافع الحفاظ على السمعة أو يقيناً باستحالة استعادة تلك الأموال[2].

والجزائر كغيرها من الدول لم تسلم هي الأخرى من ما يسمى الجريمة الالكترونية، حيث لم تسلم مواقع التواصل الاجتماعي وفضاءات تبادل المعلومات، من عملية السطو على الصور والبيانات الشخصية، واستعمالها كوسيلة للابتزاز والمساومة و التشهير، ناهيك عن استغلال بيانات الحسابات الشخصية بالإضافة إلى الاعتداء على أنظمة المعلومات، وحسب مصدر عليم لجريدة الفجر، فقد تم تسجيل أكثر من٥٠ جريمة إلكترونية في الجزائر خلال سنة٢٠١، علما أن هذا يخص عدد الحالات التي قامت بعملية التبليغ فقط، والأكيد أن البعض يرفض إيداع شكوى لاعتبارات اجتماعية وثقافية، وهو الأمر الذي جعل مصالح الدرك الوطني تتجند لحماية مستعملي الانترنت مثل مستخدمي مواقع التواصل الاجتماعي الذين يشكلون حيزا كبيرا من طبيعة استعمال هذه التكنولوجيا، كما تمت معالجة٣٨٩ جريمة الكترونية من قبل الفرق المتخصصة في مكافحة الجريمة الالكترونية التابعة للأمن الوطني، إلى جانب تسجيل٥٧ قضية في مجال جرائم الاعتداء على سلامة الأنظمة المعلوماتية[3].

٣- سبل مواجهة الجريمة الالكترونية:

١-٣-الإجراءات المتخذة على المستوى العربي والعالمي لمكافحة جرائم الانترنت والحاسوب:

أ- الشق التشريعي: سنت عدد من الدول الأوربية قوانين خاصة بجرائم الانترنت والحاسوب مثل بريطانيا وهولندا وفرنسا والدنمارك والمجر وبولندا واليابان وكندا، كما اهتمت البلدان الغربية بإنشاء أقسام خاصة بمكافحة جرائم الإنترنت، بل إنها خطت خطوة إلى الأمام وذلك بإنشاء مراكز لاستقبال ضحايا تلك الجرائم[4].

---

[1] - يوسف العربي، الهجمات الإلكترونية تزداد شراسة على الإمارات ومنظومة حماية متكاملة في المواجهة ، مقال منشور على الموقع الالكتروني لجريدة الاتحاد بتاريخ:٢٠١٦/١١/٢٧، http://www.alittihad.ae/details.php?id=60105&y=2016 ، تاريخ الاطلاع ٢٠١٧/٠٢/١١.

[2] - الاستيلاء على ٢٦.٥ مليون دولار: مصارف لبنان تتعرّض لـ٧ أنواع من الهجمات الإلكترونية!، مقال منشور على موقع (ghadi news) بتاريخ:٢٠١٦/١٢/٠١، http://ghadinews.net/Newsdet.aspx?id=27361 ، تاريخ الاطلاع ٢٠١٧/٠٢/١١.

[3] - أزيد من ٥٠٠ جريمة إلكترونية في الجزائر سنة ٢٠١٦، مقال منشور على الموقع الالكتروني لجريدة الفجر بتاريخ:٢٠١٧/٠٢/١٠، http://www.al-fadjr.com/ar/realite/352178.html ، تاريخ الاطلاع ٢٠١٧/٠٢/١١.

[4] - سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، الجريمة الالكترونية عبر الانترنيت أثرها وسبل مواجهتها، مجلة التقني، المجلد ٢٤، الإصدار ٩، ٢٠١١، ص ٤٩.

أما على مستوى الدول العربية فقد قامت الدول العربية بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وذلك بتاريخ٢٠١٠/١٢/٢١، كما أدت هذه الاتفاقية كذلك لميلاد قوانين عديدة لمكافحة ما يسمى بالجرائم الإلكترونية في السعودية والأردن وقطر والإمارات والعراق وسلطنة عمان. وصارت الاتفاقية سارية المفعول بعد تصديق الرئيس المصري عليها سنة٢٠١٤ ليكتمل نصاب الدول السبع المطلوبة لسريانها[1].

ب- الشق الأمني:

إن مواجهة مخاطر الجرائم المعلوماتية تعتمد بشكل كبير على تبني إستراتيجية أمنية- مجتمعية متكاملة، والتي تعمل فيها أجهزة مكافحة الجريمة الرسمية في الدولة جنباً إلى جنب مع أفراد المجتمع ومؤسسات القطاع الخاص، هو ما يمكن من خلاله مكافحة الأنشطة الإجرامية في الفضاء الإليكتروني والتقليل من مخاطرها والحد من انتشارها، وهذه الرؤية تتسق مع نتائج الدراسات التي أجريت في بلدان مختلفة من العالم حول التعامل مع جرائم الإنترنت، والتي أوضحت أهمية مشاركة العديد من المصادر والمؤسسات الخاصة في تحمل جزءًا من المسؤولية فيما يتعلق بمكافحة هذه الجرائم والسيطرة عليها وتلك المصادر تتمثل في[2]:

١- مزودو خدمة الإنترنت الذين يملكون القدرة على تحديد ما يعرف ب (Internet Protocol) (IP) للمشتركين، ما يتيح إمكانية مراقبة الأنشطة الخطرة على الإنترنت وتقييد اشتراك المستخدمين المنخرطين في تلك الأنشطة.

٢- المواطن العادي بدوره كذلك يمكن أن يساهم من خلال تحمل مسؤولية حماية نفسه من الوقوع ضحية لجرائم الإنترنت باقتنائه برمجيات الحماية من الفيروسات.

٣- المصارف التجارية وشركات البطاقات الائتمانية عليها أيضاً مسؤولية كبيرة في حماية عملائها من خلال تطبيق إجراءات وقائية ضد الاحتيال، وكذلك تنصيب برمجيات مراقبة خاصة على خوادمها لتعقب النشاطات غير المعتادة على حسابات العملاء ووضع أنظمة لتنبيه العميل على كل عملية تتم على حسابه.

٤- المحققين الخاصين الذين يعملون بالتنسيق مع أجهزة العدالة الجنائية يمكن أن يلعبوا دوراً مهماً في مكافحة جرائم الإنترنت.

وقد قدمت شركة « فاير آي FireEye » المتخصصة في مجال التصدي للهجمات الالكترونية المتقدمة٨ إجراءات مهمة لتفادي مخاطر تزايد الهجمات الالكترونية التي تستهدف دول الخليج العربي، بعدما كشفت عن جملة من التصورات والرؤى التحليلية بشأن مشهد الهجمات الالكترونية في مناطق أوروبا والشرق الأوسط وأفريقيا، وعلى وجه الخصوص في دول مجلس التعاون الخليجي، وتمثلت هذه الإجراءات في ما يلي[3]:

١. التوقع الدائم بأن تكون تلك الشركات مستهدفة.

٢. أنه من الممكن تخطي حدود الضوابط الأمنية المتوفرة لديها.

[1]- عزة مغازي، قانون الجريمة الإلكترونية.. التورنت يحملك إلى طرة، مقال منشور على موقع المنصة بتاريخ ٢٠١٦/٠٢/٠٤ على الرابط: https://almanassa.com/ar/story/1019 ، تاريخ الاطلاع ٢٠١٦/٠٢/١٢.

[2]- عبدالله بن فازع القرني، مواجهة جرائم الإنترنت: نحو إستراتيجية أمنية – مجتمعية متكاملة، مقال منشور على موقع جريدة الرياض بتاريخ ٢٠١٤/٠٢/٢١ على الرابط : http://www.alriyadh.com/912032 تاريخ الاطلاع: ٢٠١٧/٠٢/١٢.

[3]- ٨ إجراءات لتفادي مخاطر تزايد الهجمات الالكترونية التي تستهدف دول الخليج العربي، مقال منشور على موقع جريدة مكة، تاريخ النشر ٢٠١٦/٠٦/٠١ على الرابط: http://makkahnewspaper.com/article/147871 ، تاريخ الاطلاع: ٢٠١٧/٠٢/١٢.



٣. التأكد دائما من أن ليس هناك أي كيان تجاري بمنأى عن الهجمات.

٤. وضع إطار عمل خاص بالمخاطر ذات الصلة بالانترنت.

٥. الحصول على منصة استخبارات التهديدات الأنسب لتحسين قدرات الكشف عن الهجمات المحتملة.

٦. إنشاء خدمة الاستجابة للحوادث الطارئة وإدارتها، والتي من شأنها تمكين الشركات من اكتشافها والتفاعل مع هجمات APT بالسرعة الممكنة.

٧. تسخير التكنولوجيا المناسبة القادرة على تحديد واكتشاف هذه التهديدات الجديدة.

٨. وضع خطة استجابة واضحة والعمل على تحضيرها استعدادا للتعامل مع أي حالة اختراق.

٢-٣- التجربة العملية لدولة استونيا لمواجهة الجريمة الالكترونية: كتجربة عملية في مجال التصدي للإجرام الالكتروني نذكر على سبيل المثال « **إستراتيجية الأمن السيبراني (الأمن المعلوماتي) للفترة الممتدة من ٢٠١٤-٢٠١٧** » ، التي تبنتها دولة استونيا، وهي إستراتيجية تقوم بتحديد المخاطر التي تهدد الأمن المعلوماتي لدولة استونيا وتقدم التدابير اللازمة لإدارة هذه المخاطر، وتتولى وزارة الشؤون الاقتصادية والاتصالات مهمة توجيه سياسة أمن الانترنيت و أيضا التنسيق ما بين الأطراف المعنية بتنفيذ بهذه الإستراتيجية والمتمثلة في وزارة الدفاع الوطني، وزارة العدل، وزارة الداخلية، وزارة الخارجية، مصالح الأمن والشرطة، الجهاز المسؤول على نظام المعلومات، وزارة التعليم والبحث، ومنظمات أصحاب العمل، وتضمنت هذه الإستراتيجية مايلي[1]:

أولا- مبادئ ضمان الأمن السيبراني (الأمن المعلوماتي): اشتملت هذه الإستراتيجية على المبادئ الأساسية التالية:

- الأمن الالكتروني هو جزء لا يتجزأ من الأمن القومي، فهو يدعم سير العمل في الدولة والمجتمع، ويعزز القدرة التنافسية للاقتصاد والابتكار.

- الأمن الالكتروني مكفول من خلال احترام الحقوق والحريات الأساسية، وكذلك من خلال حماية الحريات الفردية والمعلومات الشخصية.

- يتم ضمان الأمن الالكتروني بطريقة منسقة من خلال التعاون بين القطاعين العام والخاص، مع مراعاة الترابط المتبادل بين البنية التحتية القائمة والخدمات في مجال التجارة الالكترونية.

- يبدأ الأمن الالكتروني انطلاقا من المسؤولية الفردية عن استخدام أدوات تكنولوجيات المعلومات والاتصال.

- الأولوية القصوى لضمان الأمن السيبراني هو استباق ومنع التهديدات المحتملة والتصدي بفعالية للتهديدات التي تتحقق.

- يتم دعم الأمن الالكتروني عن طريق البحث والتطوير المكثف والقادر على المنافسة دوليا.

- يُكفل الأمن الالكتروني عبر التعاون الدولي مع الحلفاء والشركاء.

ثانيا- الهدف العام من الإستراتيجية: الهدف العام من هذه الإستراتيجية هو زيادة قدرات الأمن السيبراني ، وتوعية السكان حول كيفية التعامل مع التهديدات السيبرانية، وبالتالي ضمان استمرار الثقة في الفضاء الالكتروني.

ثالثا- الأهداف الفرعية: تشتمل إستراتيجية الأمن المعلوماتي على الأهداف الفرعية التالية:

---

١ - Estonia Cyber Security Strategy 2014-2017, Ministry of Economic Affairs and Communication, Estonia 2014, p 7-12.

١- ضمان حماية نظم المعلومات الأساسية للخدمات الهامة: ويتم تحقيق هذا الهدف عن طريق الإجراءات التالية:

١-١ - تأمين أو ضمان حلول بديلة للخدمات الهامة.

١-٢ - ضمان أمن البنية التحتية وخدمات تكنولوجيات المعلومات والاتصال.

١-٣ - إدارة التهديدات السيبرانية على القطاع العام والخاص.

١-٤ - تأسيس نظام وطني لرصد أمن المعلومات .

١-٥ - ضمان الاستمرارية الرقمية للدولة.

١-٦ - تعزيز التعاون الدولي في مجال حماية البنية التحتية الحيوية للمعلومات.

٢- تعزيز مكافحة الجرائم الالكترونية: وذلك من خلال:

٢-١ - تعزيز الكشف عن الجرائم الالكترونية.

٢-٢ - رفع مستوى الوعي العام اتجاه مخاطر الانترنيت.

٢-٣ - تعزيز التعاون الدولي لمكافحة الجريمة الالكترونية.

٣- تطوير قدرات الدفاع السيبراني الوطني: عن طريق:

٣-١ - مزامنة التخطيط العسكري والاستعداد لحالات الطوارئ المدنية.

٣-٢ - تطوير الدفاع السيبراني الجماعي و التعاون الدولي.

٣-٣ - تطوير قدرات الدفاع السيبراني العسكري.

٣-٤ - ضمان مستوى عال من الوعي بشأن دور الأمن السيبراني في الدفاع الوطني.

٤- تطوير قدرات استونيا في مجال إدارة التهديدات الأمنية الالكترونية:من خلال:

٤-١ -تكوين وتأطير جيل قادم من المتخصصين في مجال الأمن المعلوماتي.

٤-٢ -المساهمة في البحوث المتعلقة بالأمن السيبراني لإيجاد الحلول الآمنة.

٤-٣ - دعم وتنمية المؤسسات التي توفر الأمن السيبراني وتقدم حلول الأمن المعلوماتي الوطني.

٥- استونيا تطور الأنشطة المشتركة بين القطاعات: عن طريق:

٥-١ - وضع إطار قانوني لدعم الأمن الالكتروني.

٥-٢ - تعزيز سياسة الأمن السيبراني الدولية.

٥-٣ - التعاون الوثيق مع الحلفاء والشركاء.

٥-٤ - تعزيز قدرة الاتحاد الأوربي.



٣-٣- تجربة الجزائر لمواجهة الجريمة الالكترونية: كخطوة أولى للحكومة الجزائرية لمواجهة ما يعرف بالجريمة الالكترونية، صدر سنة ٢٠٠٩ القانون رقم ٠٩-٠٤ المؤرخ في ٠٥ غشت ٢٠٠٩، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلا أن تجسيد بنوده على أرض الواقع ضعيف إلى حد الساعة، بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها، واقتصرت العقوبات في أغلب الأحيان على الغرامة المالي. و يتضمن القانون ١٩ مادة موزعة على ٦ فصول، أعده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية، يتضمن القانون أحكاما خاصة بمجال التطبيق وأخرى خاصة بمراقبة الاتصالات الإلكترونية وعددت الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، بالإضافة إلى القواعد الإجرائية المتضمنة تفتيش المنظومات المعلوماتية وكذا حجز المعطيات المعلوماتية التي تكون مفيدة للكشف عن الجرائم الالكترونية، و نص القانون في فصله الخامس على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، وتتكفل أيضا بتبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الالكترونية وتحديد مكان تواجدهم، كما أن هذا القانون أكد في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية من إطار مبدأ المعاملة بالمثل.[1]

وفي نفس السياق، قال رئيس الكتلة البرلمانية لجبهة العدالة والتنمية لخضر بن خلاف، في تصريح خص به «يومية السلام اليوم » أن «مشكلتنا في قوانين سنّتها الحكومة فيما يخص الجريمة الإلكترونية ولم تطبّقها»، مضيفا أن هناك مراسيم متعلقة بهذا القانون المصادق عليه سنة ٢٠٠٩، لم تصدر لحد الساعة ولأسباب مجهولة، ما جعل حسبه، معالجة القضايا من هذا الشأن تصطدم بشبه فراغ قانوني، ما أدى في عديد الحالات إلى استصدار أحكام وعقوبات تقريبية لا سند لها، كما دعا نفس المتحدث، الحكومة إلى ضرورة مراجعة موقفها تجاه هذا القانون، وقال:لا بد من إيلائه أهمية أكبر في ظل دخول الشارع الجزائري نفق الإدمان، والاعتماد الرهيب على شبكة الإنترنت وما يصاحبها من آليات وخدمات إلكترونية، فضلا عن فتح مجال السمعي البصري، الذي يمكن أن يصطدم بمثل هذه الجرائم مستقبلا، مشددا في السياق ذاته على ضرورة تشريع قوانين جديدة تكرّس العقاب الصارم لكبح مثل هذه الجرائم التي وصفها بالخطيرة والمدمّرة.[2]

الخاتمة:

إن التطورات الهائلة التي عرفتها التكنولوجيات الحديثة للإعلام والاتصال، ورغم ما وفرته من تسهيلا في أمور حياتنا، إلا أنها في المقابل فتحت الباب على مصراعيها لتطور أدوات ووسائل وسبل تنفيذ الجرائم الالكترونية، وجعلتها أكثر تعقيدا وصارت مكافحتها تبدو صعبة المنال إذا لم تتضافر جهود جميع الأطراف الفاعلة في الساحة المعلوماتية، وأمام هذا الوضع بات لزاما على حكومات الدول الإسراع في اتخاذ الإجراءات اللازمة لتطوير آليات التصدي لمثل هذه الجرائم وتعزيز التعاون الدولي في هذا المجال.

[1] – القانون رقم ٠٩-٠٤ المؤرخ في ٠٥ غشت ٢٠٠٩، مرجع سبق ذكره، ص ٥- ٨.

[2] – قاسمي.أ، 160 مليار دولار سنويا مكاسب عصابات الجريمة المنظمة عبر الإنترنت، مقال منشور على موقع يومية السلام اليوم، بتاريخ ٢٠١٤/٠١/٢٥، على الرابط: http://essalamonline.com/ara/permalink/32212.html، تاريخ الاطلاع ٢٠١٧/٠٢/١٢.



التوصيات:

- تعزيز التعاون الدولي في مجال مواجهة القرصنة والإجرام الالكتروني من خلال رسم سياسات تهدف إلى تشديد العقوبات على مرتكبي هذا النوع من الجرائم.
- تحديث وتطوير التقنيات باستمرار للتمكن من التصدي لهذه الجرائم في أقل وقت ممكن.
- تنظيم حملات توعية لمستعملي الوسائط الالكترونية (الحاسوب، الانترنيت، الهواتف الذكية ...)، وتعريفهم بحجم الخطورة التي تترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة عند استعمالهم لها.
- تعزيز وتدعيم التعاون العربي في مجال مكافحة الجريمة الالكترونية عن طريق مصادقة جميع الدول الأعضاء في جامعة الدول العربية على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وذلك من أجل درء أخطار هذه الجرائم وحفاظا على الأمن المعلوماتي للدول العربية وضمان سلامة مجتمعاتها وأفرادها.
- اتخاذ تدابير من شأنها الحفاظ على سرية المعلومات الخاصة بالحسابات البنكية وبطاقات الائتمان وغيرها من وسائل تبادل المعلومات.
- التحديث المستمر لبرامج حماية الحواسيب من الفيروسات .
- التدريب والتكوين المستمر للكوادر البشرية العاملة في مجال مكافحة الجرائم الالكترونية، واستحداث شهادات عليا متخصصة في المجالات التقنية والقانونية المتعلقة بمكافحة الجرائم المعلوماتية، وحث الجامعات والمراكز البحثية على تسليط الضوء أكثر على مثل هذه الجرائم، من خلال تكثيف الندوات والملتقيات و الأيام الدراسية حول هذا الموضوع.

المراجع:

١ - الكتب:

١- أحمد بوراس، السعيد بريكة، أعمال الصيرفة الالكترونية الأدوات والمخاطر، دار الكتاب الحديث، الجزائر.٢٠١٣

٢- أحمد سفر، العمل المصرفي الالكتروني في البلدان العربية، المؤسسة الحديثة للكتاب، طرابلس، لبنان، .٢٠٠٦

٣- السيد أحمد عبد الخالق، التجارة الالكترونية والعولمة، منشورات المنظمة العربية للتنمية الإدارية، مصر.٢٠٠٦

٤- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنيت، دار الفكر الجامعي، الإسكندرية .٢٠٠٧

٥- علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، الطبعة الأولى ٢٠١١.

٢ - المجلات:

١- سروع جو، العمل الاللتروني في المصارف بين الضروريات والمحاذير، اتحاد المصارف العربية، جمعية اتحاد المصارف العربية، المجلد ٢٠، العدد ٢٣٨، بيروت، اكتوبر.٢٠٠٠

٢- سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، الجريمة الالكترونية عبر الانترنيت أثرها وسبل مواجهتها، مجلة التقني، المجلد ٢٤، الإصدار ٩، .٢٠١١

٣- علي خليل إسماعيل الحديثي، ماهية المعاملات الإلكترونية وتبعات التنازع القانوني فيها (دراسة مقارنة)، مجلة حولية المنتدى، المنتدى الوطني لأبحاث الفكر والثقافة- العراق، المجلد ١ العدد٧، ٢٠١١.

٤- يسِّر، برنامج التعاملات الالكترونية الحكومية، مفهوم التعاملات الالكترونية، السعودية ٢٠٠٧.



٣ - المؤتمرات والملتقيات:

١- محمد صالح العادلي، الجرائم المعلوماتية (ماهيتها وصورها)، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، مسقط، سلطنة عمان،٢-٤ أفريل ٢٠٠٦.

٢- كامل فريد السالك، الجريمة الالكترونية، محاضرة ألقيت في ندوة التنمية ومجتمع المعلوماتية ٢١-٢٣ أكتوبر ٢٠٠٠، الجمعية السورية للمعلوماتية، حلب، سورية.

٣- مريم خالص حسين، الحكومة الالكترونية، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، ٢٠١٣.

٤- مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في ٢٣-٢٥/٩/٢٠١٢.

٥- موسى مسعود أرحومة، الإشكاليات الإجرامية التي تثيرها الجريمة المعلوماتي ة عبر الوطن، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ٢٠٠٩.

٦- يونس عرب، صور الجرائم الالكترونية واتجاهات تبويبها، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان،٢-٤ ابريل ٢٠٠٦.

٤ - الرسائل الجامعية

١- صغير يوسف، الجريمة المرتكبة عبر الانترنيت، رسالة ماجستير في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، ٢٠١٣.

٥ - القوانين والتشريعات:

١- القانون الاتحادي رقم (1) لسنة ٢٠٠٦، المؤرخ في ٣١-٠١-٢٠٠٦، المتعلق بقانون المعاملات والتجارة الإلكترونية، الجريدة الرسمية رقم ٤٤٢، الفصل الأول، المادة ١، الفقرة ٢٦.

٢- المرسوم السلطاني رقم (٦٩-٢٠٠٨) ، المؤرخ في ١٧-٠٥-٢٠٠٨، المتعلق بقانون المعاملات الإلكترونية، الفصل الأول، المادة ١،الفقرة ٠٤ .

٣- قانون المعاملات الالكترونية السوداني المؤرخ في ١٤-٠٦-٢٠٠٧، الفصل الأول، المادة ٢، الفقرة ١٤.

٤- القانون رقم ٠٩-٠٤، المؤرخ في ٠٥ غشت ٢٠٠٩، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم ٤٧.

٦ - مواقع الانترنيت:

١- موقع ويكيبيديا: https://ar.wikipedia.org/wiki/تجارة_الكترونية

٢- بوابة الأكاديمية العربية البريطانية للتعليم العالي : http://www.abahe.co.uk/dictionary-e-commerce.html

٣- مركز دراسات الحكومة الالكترونية: http://www.egovconcepts.com

٤- هيئة تقنية المعلومات لسلطنة عمان: http://www.ita.gov.om/ITAPortal_AR/Info/FAQ_eGovernmen.aspx

٥- مدونة الدكتور حافظ الشجي: http://alshihi.blogspot.com/2009/10/blog-post_20.html

٦- المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية: http://democraticac.de/?p=35426

٧- موقع كنانة أونلاين: http://kenanaonline.com/users/ahmedkordy/posts/320920

٨- موقع قناة الجزيرة ، قسم علوم وتكنولوجيا :
http://www.aljazeera.net/news/scienceandtechnology/2015/4/6

٩- المركز العربي لأبحاث الفضاء الالكتروني : http://accronline.com/article_detail.aspx?id=7509

١٠- موقع قناة الجزيرة الالكتروني http://www.aljazeera.net/knowledgegate/newscoverage/2015/1/5/

١١- موقع أرقام ديجتال: http://digital.argaam.com/article/detail/112326

١٢- موقع: http://www.arageek.com/tech/2016/12/25/2016-hacking-operations.html

١٣- موقع باب : http://bab.com/Node/275623

١٤- موقع« عربية SKY NEWS » : http://www.skynewsarabia.com/web/article/724420

١٥- الموقع الالكتروني لجريدة الاتحاد http://www.alittihad.ae/details.php?id=5035&y=2016&article=full

١٦- موقع الخليج الجديد http://thenewkhalij.org/ar/node/43159

١٧- موقع (ghadi news) http://ghadinews.net/Newsdet.aspx?id=27361

١٨- جريدة الفجر http://www.al-fadjr.com/ar/realite/352178.html

١٩- موقع المنصة : https://almanassa.com/ar/story/1019

٢٠- موقع جريدة الرياض : http://www.alriyadh.com/912032

٢١- موقع جريدة مكة : http://makkahnewspaper.com/article/147871

٢٢- موقع يومية السلام اليوم : http://essalamonline.com/ara/permalink/32212.html

٧ - المراجع الأجنبية:

١ - FFIEC, Federal Financial Institutions Examination Council, B-Banking, IT Examination Handbook, August 2003.

2- cyber security economy predictions 2017-2021,cybersecurity ventures 2016 .

3- Estonia Cyber Security Strategy 2014-2017, Ministry of Economic Affairs and Communication, Estonia 2014.



أليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا

د. حسين نوارة كلية الحقوق و العلوم السياسية –

جامعة مولود معمري تيزي وزو- الجزائر

مقدمة

عرف العالم في الأعوام الأخيرة تطورا مذهلا في المجال العلمي والتقني والتكنولوجي والرقمي لاسيما في مجال تكنولوجيات الإعلام والاتصال وذلك بسبب ظهور الانترنت والمواقع الاليكترونية ووسائل أخرى حديثة ومتطورة. وعليه فالتكنولوجيا والتطور العلمي والتقني مهما كان نوعه يمكن أن يكون سلاح ذوا حدين ، الأمر الذي دفع بالمشرعين لتنظيم هذه المجالات بما يخدم حقوق الإنسان بمختلف أنواعها لا الاعتداء عليها، وتأطير كل طرق استخداماتها، لاسيما استخدام الانترنت كأحدث وسلة في مجال الاتصال والتواصل ونخص بالذكر" **مواقع الانترنت**" أو مواقع التواصل الاجتماعي والتصدي لما ينتج عنها من مساس بالحقوق الخاصة للأفراد[1].

إن تطوير الحواسيب الرقمية وتكنولوجيا الشبكات[2] ، وبشكل خاص الخدمات على مواقع الإنترنت أتاح نقل النشاط الاجتماعي والتجاري والسياسي والثقافي والاقتصادي من العالم المادي إلى العالم الافتراضي أي "**البيئة الالكترونية**"، ويوماً بعد يوم تتكامل الشبكات العالمية للمعلومات مع مختلف أنشطة الحياة ، وبنفس الوقت فان التطور الثقافي في توظيف التقنية رافقه توجه واسع بشأن حماية خصوصية الأفراد.

ففي العالم الرقمي وعالم شبكات المعلومات العالمية يترك المستخدم آثار ودلالات كثيرة تتصل به بشكل سجلات رقمية حول الموقع الذي زاره والوقت الذي قضاه على الشبكة والأمور التي بحث عنها والمواد التي قام بتنزيلها والوسائل التي أرسلها والخدمات والبضائع التي قام بطلبها وشرائها أو التي قام بعرضها والدعاية لتسويقها، وهي سجلات تتضمن تفاصيل دقيقه عن شخصية وحياة وهوايات وميول المستخدم الشخصية على الشبكة وهي سجلات مؤتمنة ذات محتوى شخصي يتصل بالفرد. بحيث ينتج عن التصفح والتجول عبر الأنترنت أن المستغل يترك لدى الموقع الزار كمية واسعة من المعلومات الشخصية على الرغم من أن جزءا من هذه المعلومات فقط لازم لإتاحة الربط بالإنترنت والتصفح ، وبمجرد الدخول إلى

---

[1] – د/ نوارة حسين ، مظاهر اعتداء مواقع الانترنت على الحياة الخاصة، الملتقى الوطني حول تأثير التطور العلمي و التقني على حقوق الإنسان، كلية الحقوق، جامعة بجاية ، ١٩–٢٠ نوفمبر ٢٠١٣، ص ١.

[2] – لقد تطرقت منظمة التعاون الاقتصادي و التنمية عند تعريفها للتجارة الإليكترونية في تقريرها الذي صدر في سنة ١٩٩٨ للمشاكل المتعلقة بحماية الموقع الاليكتروني و اسمه و عنوانه على الشبكة العالمية ، وكل حقوق الملكية الفكرية و القانون الواجب التطبيق على التصرفات القانونية التي تتم من خلالها .

–أنظر /خالد ممدوح إبراهيم ، إبرام العقد الاليكتروني، دراسة مقارنة ، دار الفكر الجامعي ،الاسكندرية ،٢٠١١ ص ٤٥.

صفحة الموقع فان معلومات معينه تتوفر عن الزبون وهي ما يعرف بمعلومات رأس الصفحة وهي التي يزودها الكمبيوتر المستخدم للكمبيوتر الخادم الذي يستضيف مواقع الأنترنت ، وهذه المعلومات قد يكون في استخدامها أثر سلبي على عدة مستويات وأهمها على مستوى حقوق صاحبها بصفة خاصة وحقوق الإنسان عموما ، وذلك رغم الايجابيات المتعددة التي يمكن إحصاءها من جراء التعامل بالآليات والتقنيات التكنولوجية المتطورة.

وعليه في الاستغلالات المختلفة للشبكة العنكبوتية ما يدل على أن مظاهر التكنولوجيا و التطور العلمي والتقني مهما كان نوعها يمكن أن يكون في سوء استعمالها من النتائج السلبية التي تجعلنا نصفها بالسلاح ذوا الحدين .

على العموم، استفحلت الجريمة الجمركية وزاد حجمها في مختلف المجتمعات، وامتد الاعتداء فيها الى جميع نواحي الحياة ، ومست حتى مظاهر الحياة الخاصة ، من خلال هذه الدراسة نتساءل عن **أليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة اليكترونيا؟.**

المبحث الأول :

الاطار المفاهيمي لجريمة الاعتداء على الحياة الخاصة إليكترونيا

جعلت الشريعة الإسلامية حق الشخص في الحياة قاعدة من قواعدها، و حقه في خصوصية حياته أساسها، فحرم كل أشكال المساس بها أو الاعتداء عليها، فجعل حمايتها من الواجبات و الامتناع عن ايذائها من المفروضات، وكانت حرمة الحياة والمسلئن، والمعلومات السرية، والاخبار العائلية والاسرية و المراسلات والمحادثات و المعتقدات و الميول الدينية و السياسية و ...غيره، خاصا بالشخص، فسوّت ولم تميّز بين الآليات المتبناة للاعتداء سواء بالسمع، أو بالالتقاط الصور أو التجسس أو ....أي شكل آخر طالما في الاخير نتيجة الفعل هو المساس بالحرمة. لكن مع تطور كل مناحي الحياة تغيّرت الرؤى و المواقف، حيث تم عصرنة أساليب العيش فتغيّرت معها مفاهيم كثيرة.

وأمام اشكالية الرؤى الجديدة للحياة العصرية ، نتطرق لمفهوم الحق في الحياة الخاصة و لمضمونه في المبحث الاول.

المطلب الاول : تعريف الحياة الخاصة

لم يرد للحياة الخاصة تعريف جامع ومانع لا في الفقه والقضاء ولا في التشريع، ومرّد ذلك هو صعوبة وضع تعريف موحد للمصطلح، لذلك تعد محاولة إيجاد تعريف للحياة الخاصة أمرا بالغ الصعوبة حيث يترتب على وضع هذا التعريف تحديد العناصر المشكلة له ، فضلا عن أنها فكرة مرنة وغير محددة، وتختلف باختلاف الزمان والمكان والأشخاص. كما أنه يصعب وضع تعريف محدد للحياة الخاصة ذلك أن التعريف لا يكون إلا لفكرة ثابتة ومحددة ، أما الحياة الخاصة فهي فكرة مرنة ومتغيرة ونسبية ، غير أنه رغم عدم تحديد مدلولها والإلمام بمعناها إلا أن ذلك لا يمنع أنها تتمتع بالحماية القانونية الكاملة في العديد من التشريعات حتى تظل منأى عن تدخل الغير وعن العلانية. بل إن القضاء قد استقر على ضرورة أن تحاط الحياة الخاصة بسياج وحائط يحميها من تدخل الغير واطلاعه عليها.

إن هذه الصعوبة في تحديد تعريف للخصوصية راجع لارتباطها بالانتماءات الدينية والعادات والقيم في المحيط الذي يعيش فيه الشخص[1]. فنجد أنه في التشريعات والقوانين الدولية لا يُذكر فيها تعريف معين للخصوصية، وإنما تكتفي بوضع نصوص تكفل حماية هذا الحق وتعدِد صور الاعتداء عليه.



و قد تعتبر قوانين حفظ الخصوصية في العديد من الدول محدودة المجال، فعلى سبيل المثال القوانين المرتبطة بتحصيل الضرائب، والتي تتطلب عادةً مشاركة البيانات الشخصية المالية من إيرادات وديون.

وقد تتعارض قوانين حفظ الخصوصية في بعض الدول مع قوانين حرية التعبير. ويصف بعض الباحثين الاقتصاديين وعلماء النفس بأن الإفصاح عن بعض المعلومات الشخصية، لهدف الدخول في المسابقات والمنافسات، هي "**تضحية طوعية**"، حيث أن البيانات الشخصية التي يتم الكشف عنها طوعياً قد تتعرض لاحقاً للسرقة أو تُستخدم لأهداف غير التي جُمِعت لها، كجرائم سرقة الهوية.

كذلك في اطار تعريف الحق في الحياة الخاصة نذكر على سبيل المثال تعريف المحامي يونس عرب للحياة الخاصة كما يلي: " **الحياة الخاصة للإنسان تشمل الحق في العيش مع ذاته و أسرته في هدوء وسكينة، و الحق في السرية المهنية ، وسرية المراسلات والمحادثات، حرمة المساكن وحرية الاعتقاد والفكر، المسألة العاطفية والعائلية، والروحية والمالية ..الخ ، وهي من المظاهر الاجتماعية الضرورية لكل إنسان. وجزءاً لا يتجزأ من الوجود الإنساني تجب حمايته بكل قوة من التعسف والاعتداء أ ياً كان الشخص المعتدي وبغض النظر عن المعتدى عليه أو الوسيلة المستعملة في الاعتداء** ".[1]

إن الحياة الخاصة للفرد تتحدد حسب المجتمع الذي ينتمي إليه ذلك الفرد أي حسب أخلاق و ثقافة و عادات المجتمع ، لذلك تعتبر الحياة الخاصة" **فكرة نسبية**" محكومة ومقيدة بحكم قيم و قواعد السلوك و القانون الأخلاقي لكل مجتمع ، لذلك تكون حتى صور الاعتداءات التي تقع على الحق في الحياة الخاصة مقيّد و متوقفة على نفس العناصر ، بل و بالنسبة للاعتداءات التي تقع على نفس الحقوق على الشبكة العنكبوتية أو على مواقع الانترنت أو بالوسائل التكنولوجية المتطورة تبقى أيضا متوقفة على درجة هذا التقدم ، لذلك لا نستطيع مقارنة صور الاعتداء على الحياة الخاصة في الجزائر بتلك التي يتعرض لها الإفراد في الولايات المتحدة الأمريكية فأبعاد الخصوصية و عناصرها في المجتمعات العربية مختلفة إلى حدّ بعيد عن تلك المعروفة في المجتمعات الغربية.

ومن حيث تعريف الحياة الخاصة فلا نميّز بين تلك المنتهكة" **بوسائل الاعتداء المادية التقليدية** "و تلك التي يتم انتهاكها" بوسائل الاعتداء الاليكترونية " أي باستخدام "**الوسيط الاليكتروني**"، لان الاختلاف يمس صور الاعتداء لا الحق المعتدى عليه . .

و من جهة أخرى، ارتبط مفهوم الخصوصية – في العديد من الكتابات والبحوث - بمصطلح حماية البيانات و معالجتها مما جعلها تُضبط في إطار حماية البيانات الخاصة، نذكر على سبيل المثال التعريف الذي صدر عن وزارة الداخلية السعودية عرفت البيانات الشخصية، في مذكرتها للمبادئ الأساسية لأمن المعلومات وخصوصيتها، كالتالي: " **كل ما يتعلق بالحياة**

---

[1]- حتى النظام الإسلامي استمد أصول مبدأ الحق في حرمة الحياة الخاصة من الأديان السماوية السابقة عليه، أو من القانون ال روماني، ومن النظم التي كانت سائدة في الإمبراطوريتين الرومانية والفارسية، وقد صرح بعض الباحثين بوجود تشابه بين مدونة جستينيان والشريعة الإسلامية، وأش ار أن القانون الروماني قد تسربت قواعده إلى الإسلام كما ذهب بعضهم إلى أن الشريعة الإسلامية ليست إلا القانون ا لروماني للإمبراطورية الشرقية، معدلا وفق الأحوال السياسية في الممتلكات العربية.

انظر: بسيوني عادل، تاريخ القانون المصري، مصر الإسلامية، مكتبة نهضة الشرق، القاهرة، ١٩٨٥،ص٩٦.

[1] – المحامي يونس عرب

المصدر http://www.arab-elaw.com/show_similar.aspx?id=20

الخاصة للإنسان كهويته وجنسيته واتجاهاته وميوله ومعتقداته وتعاملاته المالية والبنكية، فهي معلومات ترتبط بشخص مُعرَّف أو قابل للتعريف".

و تعريف آخر صدر للمصطلح نفسه عن مكتب خبراء البيت الأبيض للعلوم والتقنية التالي: " **حق الفرد في الخصوصية هي حقه على الاختيار الشخصي فيما يريد مقاسمته مع الآخرين من أفكاره وعواطفه والحقائق المتعلقة بحياته الشخصية**" .[1]

وما يمكن ذكره كتعريف للحق في الخصوصية حسب مجتمعنا العربي الإسلامي ما يلي: " **إن الحق في الحياة الخاصة هي حق الشخص في أن يحترم الغير كل ما يعد من خصوصياته مادية كانت أو معنوية أو تعلقت بحرياته ، على أن يتحدد ذلك بمعيار الشخص العادي و وفقا للعادات و التقاليد و النظام القانوني القائم في المجتمع و مبادئ الشريعة الإسلامية** "[2] .

المطلب الثاني : تكريس مبدأ الحماية القانونية للحياة الخاصة ضد الاعتداءات الاليكترونية:

تعتبر "**الحياة الخاصة**" أو ما يطلق علها "**الحق في الخصوصية** " أقدم الحقوق التي أقرتها المجتمعات للأفراد

لأنها مرتبطة ارتباطا وثيقا بحرية الفرد وحقوقه الأساسية الخاصة كما سبق قوله أعلاه ، حيث قرّرت لها كل التشريعات الحماية القانونية من كل أشكال الاعتداء التي يمكن أن يتعرض لها الفرد، و قد تطور هذا الحق و امتد نطاقه ليشمل حماية كل عناصر الحياة الخاصة للشخص من كافة أوجه الاعتداء و التدخل في حياته أيا كان مظهرها أو طبيعتها، بحيث تمتد إلى حمايته من أشكال" **الاعتداء الاليكتروني**" الذي يقع بموجب الوسائل الحديثة الرقمية و الاليكترونية و عبر شبكة الانترنت و بالخصوص في إطار" **المواقع الاليكترونية أو أسماء النطاق** "[3]

فبسبب التطور التقني و التكنولوجي الذي شهده هذا العصر أصبحت الحماية القانونية للحق في الحياة الخاصة المنصوص عليها في النصوص القانونية التقليدية لا سيما قوانين العقوبات المقصّرة بسبب كون التحديات التي تواجهها من نوع جديد في عصر المعلوماتية الرقمي و في عصر العولمة والعصرنة، وذلك لعدم قدرة و كفاية الوسائل و الآليات التي قررتها للحماية ضد الأنواع الجديدة للاعتداء لاسيما بسبب صعوبة تحديد هوية المعتدي على المواقع الاليكترونية ، و لان نطاق الاعتداء هو الوسيط الاليكتروني الذي تتم فيه كل أركان الجريمة و هو عالم " **افتراضي**" و غير ملموس .

غير أنه امام استفحال ظاهرة الاعتداءات الاليكترونية على الحق في الخصوصية والجريمة الاليكترونية عموما، تم تكريس حمايتها تشريعيا أولا، و دوليا ثانيا.

أولا - التكريس التشريعي للحق في الحياة الخاصة:

من حيث المبدأ الحماية القانونية للحقوق المرتبطة بالحياة الخاصة أو للخصوصية مبدأ دستوري أقرته معظم

---

[1] – ماهية الحق في الخصوصية ،٢٥/ ١١/٢٠٠٨ ، المصدر http://www.startimes.com/?t=13100755

[2] – جعفر محمود المغربي ، حسين شاكر عساف ، المسؤولية المدنية عن الاعتداء على الحق في الصورة بواسطة الهاتف المحمول ، القانونية التي تتم من خلالها ، دار الثقافة للنشر و التوزيع ، عمان ،٢٠١٠ ، ص ٣٣ .

[3] – جعفر محمود المغربي ، حسين شاكر عساف ، مرجع سابق ، ص ٣٨ .

الدساتير و التشريعات العالمية [1]و منهم الدستور الجزائري الذي كرس حماية حق الإنسان في حياته الخاصة في دستور١٩٩٦ في المادة ٤٠ منه التي تنص على أنه :" **تضمن الدّولة عدم انتهاك حرمة المسكن. فلا تفتيش إلاّ بمقتضى القانون، وفي إطار احترامه. ولا تفتيش إلاّ بأمر مكتوب صادر عن السّلطة القضائية المختصّة.**" ويضيف الدستور الجزائري في المادة٣٩ على انه :" **لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه، ويحميهما القانون. سرّية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة** ".

و قد كرس المشرع هذا الحق في المادة٣٠٣ مكرر من قانون العقوبات المعدل بالقانون رقم٢٣٠٦ المؤرخ في ٢٠٠٦/١٢/٢٠ [2] التي نصت على ما يلي :"**يعاقب بالحبس من ستة أشهر إلى٣ سنوات كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص ، بأي تقنية كانت و ذلك :**

١-التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية ، بغير إذن صاحبها أو رضاه

٢- التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص ، بغير إذن صاحبها أو رضاه".

كما وردت لهذه النصوص الدستورية بعض النصوص الخاصة المجسدة للمبدأ العام من خلال التطرق بصفة خاصة إلى حماية الحق في الحياة الخاصة.

و من بينها ما ورد في القانون العضوي رقم١٢-٠٥ المؤرخ في١٢/٠١/٢٠١٢ و يتعلق بالصحافة في المادة ٢:"**يمارس نشاط الإعلام بحرية في إطار أحكام هذا القانون العضوي و التشريع و التنظيم المعمول بهما و في ظل احترام:**

-الدستور وقوانين الجمهورية .

-الدين الإسلامي و باقي الأديان .

-الهوية الوطنية و القيم الثقافية للمجتمع...

-حق المواطن في إعلام كامل و موضوعي

-سرية التحقيق القضائي .

- كرامة الإنسان و الحريات الفردية و الجماعية" [3].

---

[1] – و على سبيل المقارنة ، نجد أن المشرع السوري أقر عدداً من النصوص القانونية والدستورية تؤكد على حماية حق الإنسان في حياته الخاصة، حيث قرر عقوبة في المادة ٥٥٧ من قانون العقوبات السوري على خرق حرمة المنازل خلافاً لإرادة صاحبها بالحبس مدة لا تتجاوز ستة أشهر . وأجاز في المادة ٥٢من القانون المدني ما يلي " **لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة للشخصية أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر** ". كما كرس حماية هذا الحق في الدستور السوري النافذ حالياً وأفرد عدداً من المواد لحماية بعض مظاهر الحياة الخاصة، فنص في المادة ٢٥ منه علي :" **الحرية حق مقدس وتكفل الدولة للمواطنين حريتهم الشخصية وتحافظ على = =كرامتهم وأمنهم**" وكذلك نص في المادة٣١ منه على : " **المساكن مصونة لا يجوز تفتيشها أو دخولها إلا في الأحوال المبينة في القانون** " كما نص في المادة ٣٢ على " **سرية المراسلات البريدية والاتصالات السلكية مكفولة وفق الأحكام المبينة في القانون**" .

[2] – القانون رقم ٠٦-٢٣ المؤرخ في ٢٠٠٦/١٢/٢٠/ يتضمن تعديل قانون العقوبات ، ج رعدد٨٤.

[3] – قانون عضوي رقم ١٢/٠٥ ، مؤرخ في ٢٠١٢/٠١/١٢، يتعلق بالصحافة.

وهنا حماية للحياة الخاصة من تجاوزات الصحافة التي تبرر كل تصرفاتها التي تلحق الضرر بالغير على أساس مبدأ حرية الإعلام .

كما نص القانون رقم٠٩-٠٤ المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة٤ على أنه:"**يمكن القيام بعمليات المراقبة المنصوص عليها في المادة٣ ...للوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة، في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية...وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات، بالنسبة للمساس بالحياة الخاصة للغير**"[1]، وهو نص في غاية الأهمية بالنسبة لمبدأ الحق في الحياة الخاصة لما يحمله من ضمانات للأفراد على وجه العموم.

لكن مؤخرا، حاول المشرع الجزائري أن يتماشى مع ما هو معمول به في مجال محاربة الإجرام ألمعلوماتي وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية، بموجب القانون رقم٠٤-١٥ المتضمن تعديل قانون العقوبات، خاصة بسبب التزايد اللا متناهي للاعتداءات على الأنظمة المعلوماتية بتطور آليات الاتصال وظهور مواقع الاليكترونية والانترنت، حيث يتضمن التعديل الأخير لقانون العقوبات في الفصل الثالث من الباب الثاني من الكتاب الثالث قسم سابع مكرر عنوانه "**المساس بأنظمة المعالجة الآلية للمعطيات**"، ويشمل المواد من٣٩٤ مكرر إلى٣٩٤ مكرر٧.

حيث نصت المادة٣٩٤ مكرر قانون العقوبات: "**يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من ٥٠٠٠٠ إلى ١٠٠٠٠٠ دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك**"، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "**تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من ٥٠٠٠٠إلى ١٥٠٠٠٠ دج**".[2] وذلك مهما كانت قاعة المعلوماتية أو طبيعتها لذلك يمكن أن تندرج ضمن هذه الاعتداءات تلك التي تمس ببعض صور الحياة الخاصة.

ونصت المادة٣٩٤ مكرر٢ على أنه: "**يعاقب...كل من يقوم عمدا وعن طريق الغش بما يأتي** :

١-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم .

٢-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم" .

و تضيف المادة٣٩٤ مكرر٦ أنه بالإضافة إلى العقوبات الأصلية أي الحبس و الغرامة و بالاحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية : "**يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم ، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها** " .

[1] – قانون رقم ٠٩/٠٤ ، مؤرخ في ٢٠٠٩/٠٨/٠٥ ،يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، ج ر عدد ٤٧ مؤرخة في ٢٠٠٩/٠٨/١٦ .

[2] – القانون رقم ٠٤/١٥ المؤرخ في ٢٠٠٤/١١/١٠ ، متضمن تعديل قانون العقوبات، ج ر عدد ٧١ .



ثانيا- التكريس الدولي للحق في الحياة الخاصة:

لقد دفع التطور المذهل لوسائل الاعتداء على الحياة الخاصة للإنسان العديد من المفكرين وعلماء القانون والناشطين في مجال حقوق الإنسان إلى البحث جدياً عن السبل الكفيلة لحماية الحياة الخاصة للإنسان بصفة عامة لذلك تضافرت الجهود الدولية والإقليمية لحماية الخصوصية، فتضمنه الإعلان العالمي لحقوق الإنسان وأولاه أهمية خاصة، إذ نص في المادة ١٢ منه على أنه: " **لا يجوز تعرّض أحد لتدخل تعسفي في حياته الخاصة أو شؤون أسرته أو مسكنه أو مراسلاته...ولكل شخص الحق في أن يحميه القانون من مثل ذلك التدخل".**

وأكد العهد الدولي الخاص بالحقوق المدنية والسياسية على حماية هذا الحق في المادة ١٧ منه:" **لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني لتدخل في خصوصياته، أو شؤون أسرته أو بيته أو مراسلاته، ومن حق كل شخص أن يحميه القانون من مثل ذلك التدخل".**

كما أصدرت الجمعية العامة للأمم المتحدة القرار رقم ٢٢٠٠ لسنة ١٩٦٦ يتعلق بالاتفاقية الدولية للحقوق المدنية والسياسية وقد نصت هذه الاتفاقية في المادة (١٧) منها على:" **لا يجوز التدخل بشكل تعسفي أو غير قانوني في المسائل الخاصة بأي شخص أو عائلته أو بمسكنه أو بمراسلاته، كما لا يحوز التعرض بشكل غير قانوني لما يمس شرفه وسمعته. لكل شخص الحق في حماية القانون ضد مثل هذا التدخل أو التعرض"** .

كما أن المشروع الإسلامي التاسع الصادر عام ١٩٩٠ أكد على:" ب - **وللإنسان الحق في الاستقلال بشؤون حياته الخاصة في مسكنه وأسرته، ولا يجوز التجسس أو الرقابة عليه أو الإساءة إلى سمعته، وتجب حمايته من كل تدخل تعسفي. "** .

وكان لمجلس أوربا دور كبير في عقد الاتفاقية الأوربية لحقوق الإنسان والحريات العامة لعام ١٩٥٠، حيث أوجبت المادة ٨"من هذه الاتفاقية على حماية الحياة الخاصة بالنص على حماية الأفراد من التدخل والاعتداء على حياتهم الخاصة وحياة أسرهم. كما قررت المادة ١٠"من هذه الاتفاقية على وجوب حماية حق الوصول ونقل المعلومات، بالإضافة إلى ذلك فقد كان للاتحاد الأوربي دور كبير في حماية الحق في الخصوصية، إذ صدر عن الاتحاد عدة تعليمات بهذا الشأن منها

-التعليمات المتعلقة بحماية الأفراد من أنشطة خزن ونقل البيانات.

-التعليمات المتعلقة بحماية الأفراد من أثر التطور التقني لمعالجة البيانات

- التوجيه الأوربي رقم ٨٥ الصادر من البرلمان الأوربي في سنة ٢٠٠٢ والمتعلق بالمعالجة الآلية للبيانات وحماية الحياة الخاصة[1].

المبحث الثاني :

نطاق اعتداء الجريمة الاليكترونية على الحياة الخاصة ونظام المسؤولية عن ذلك

ام من المسائل البالغة الاهمية التي يجدر بنا التطرق اليها هي تحديد نوع الاعتداءات التي يمكن أن تمس بالحياة الخاصة و التي تتم عبر الوسيط الاليكتروني، وتتماشى مع طبيعة البيئة الاليكترونية التي تساعد و تسهل على الجاني اتيان الفعل و اكتمال اركان الجريمة. ثم القانون الواجب التطبيق على الجريمة ونظام المسؤولية الذي يتم ردع الفعل على أساسه، نظرا

[1] – انظر : **د/** نوارة حسين ، مرجع سابق، ص ١٠ وما بعدها.

لعدم وجود قانون خاص بالجريمة الاليكترونية و نخص الذكر القانون الجزائري ، لان دول لكثيرة كانت سباقة في ارساء نظامها الكامل و الخاص بالجريمة الاليكترونية لتأمين التعاملات الاليكترونية من جهة وحماية الخصوصية من جهة ثانية مثل ما هو معمول به في القانون الامريكي.

وعليه نتطرق في المطلب الاول لنطاق اعتداء الجريمة الاليكترونية على الحياة الخاصة، و في المطلب الثاني لنظام المسؤولية الناشئة عن الاعتداء.

المطلب الاول : نطاق اعتداء الجريمة الاليكترونية على الحياة الخاصة

من خلال ما سبق قوله يمكن أن نستنتج أن الحق في الخصوصية أو الحياة الخاصة اقترنت كحد أدنى بالعناصر الأساسية المشكلة للحق في الحياة الخاصة من جهة، وصور الاعتداء الالكتروني على الحياة الخاصة قد وردت عليه بعض الاستثناءات نتناولها فيما يلي:

- أولا: عناصر الحق في الحياة الخاصة: تتمثل في

* خصوصية المعلومات و تشمل كل البيانات الخاصة كالمعلومات بطاقات الهوية ، و المعلومات الواردة في البطاقات الاليكترونية البريدية ، المهنية ...

*الخصوصية الجسدية و المادية ، كالنتائج التي تنتج عن الفحوصات الطبية عن المخدرات ، الايدز ، الجينات ...، تحليل ADN.

*خصوصية الاتصالات و المراسلات الهاتفية السلكية و غير السلكية ، و البريد الاليكتروني ، وسرية المكالمات الصوتية عبر الهواتف النقالة... [1].

* الخصوصية الإقليمية والمكانية كالحق في عدم اقتحام المساكن و التعرض للتفتيش أو التعرض لاي شكل من

أشكال لانتهاك في المنازل و مكان العمل .

وبالرجوع إلى القانون الجزائري فيما يخص نطاق الحق في الحياة الخاصة المنتهكة عبر مواقع الانترنت، أو حتى من الاعتداءات الاليكترونية الأخرى و التي تتم بموجب الوسائل الاليكترونية و الرقمية، فلا نجد لها أثر ، فالمشرع من حيث النص لم يواكب التطورات في مجال المعلوماتية أو في المجال الرقمي الاليكتروني ، فالمشرع اكتفى بإقرار المبدأ في حماية الخصوصية في شكله العام دون التعرض للوسيلة المعتمدة في تحقيق الاعتداء ، فالحماية قائمة مهما كانت أشكال الاعتداء لأن الاعتداد في هذه الحالة يكون بوجود الخطأ و الضرر الذي يلحق أحد جوانب الحياة الخاصة

وعموما لا يوجد أي دستور عربي ينظم مظاهر حماية خصوصية المعلومات أو البيانات الشخصية أو مسائل معالجتها الالكترونية على نحو ما هو منصوص عليه في دساتير الدول الأجنبية، مع خلوها من المبادئ التي قد تحد على الأقل من انتهاكات هذا الحق ، لأن التجربة حاليا جديدة ومحتشمة، باستثناء النصوص التي تكفل الحق فيحماية الحياة الخاصة كمبدأ عام والتي تخضع لنوع من التطويع لتكون قابلة التطبيق على الجرائم الاليكترونية، لان هذه الاخيرة في أصلها مثل الجريمة الاليكترونية وتختلف عنها في كونها مرتكبة عبر الوسيط الاليكتروني.

[1] – انظر : د/ نوارة حسين ، مرجع سابق.

ثانيا- صور الاعتداء الالكتروني على الحياة الخاصة و الاستثناءات التي ترد عليها :

لقد صنع التقدم العلمي و التكنولوجي و التقني ، الاليكتروني و الرقمي طفرة في مجال وسائل الإعلام و الاتصال والتواصل بحيث أصبح العالم قرية صغيرة محدودة المعالم ، بحيث ترتب عن ذلك تأثير كبير على تطور الحق في الحياة الخاصة بسبب البحث عن وسائل و آليات جديدة لمواجهة الأخطار التي تهدد هذا الحق ومن خلال سن قوانين جديدة قادرة على تنظيم هذا الحق الذي يتم تداوله عبر الوسائل الحديثة للاتصال و التواصل و حمايته بصفة فعالة أمام التحديات التي يفرضها واقع العصر الحديث [1].

١ - صور الاعتداء الالكتروني على الحياة الخاصة :

إن المخاطر التي تهدد الحياة الخاصة كثيرة و متعددة أفرزتها مختلف التطورات التي حدثت بظهور شبكة الانترنت التي توسعت من خلالها صور التواصل في المجتمع لاسيما في المواقع الاليكترونية بين الأفراد هذا من جهة ، و من جهة أخرى بسبب توسع نشاط تدخل الدولة في جمع البيانات عن الأفراد وتخزينها من خلال استغلال الأنظمة المعلوماتية المستحدثة [2]. إن أهم المخاطر التي تهدد الحياة الخاصة في ظل ظهور المواقع الاليكترونية و تطور مجال المعلوماتية و باكتشاف العقول الاليكترونية كثيرة [3]، لكن نذكر منها علىسبيل المثال التالية:

* الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها وجعلها غير قابلة للاستخدام الحصول على المعلومات السرية للمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها.

* التصنت على المكالمات الخاصة و تسجيلها لإذاعتها على المواقع بهدف الابتزاز.

* التقاط الصور الخاصة دون الحصول على موفقة صاحبها بواسطة كاميرات الفيديو و كاميرات المراقبة السرية و عرضها على المواقع الابتزاز أو التشويه بالسمعة.

* التجسس على الأسرار الخاصة و التجسس على الاتصالات والمراسلات وسريتها عن طريق المراقبة الالكترونية بالأقمار الصناعية والكاميرات الرقمية المحولة عن طريق الهواتف المحمولة و كشفها عبر الفايسبوك أو على المواقع الاليكترونية لتحقيق الربح السريع.

* نشر وإعلان و التلاعب في البيانات الشخصية أو محوها عن طريق أشخاص غير مرخص لهم بذلك في وسائل الإعلام والاتصال المختلفة دون موافقتهُ الصريحة أو الضمنية.

---

١ – عندما يستخدم الأفراد مواقع الانترنت يتوقعون قدرا من الخفية في نشاطهم أكثر مما هو في العالم المادي الواقعي ، لكن في الحقيقة يمكن ملاحظة وجودهم ومراقبتهم من قبل الآخرين ، فالانترنت عبر نظم الخوادم ونظم إدارة الشبكات تصنع قدرا كبيرا من المعلومات عند كل وقفة في فضاء الشبكة . وهذه البيانات قد يتم اصطيادها ومعرفتها من قبل صاحب العمل عند استخدامه للشبكة أو غيره من القراصنة ، وقد تجمع من قبل المواقع المزارة نفسها ، فان جمع شتات معلومات وسلوكيات معينة قد يقدم أوضح صورة عن شخص لم يدرك كشف أي من تفاصيل ما تضمنته .

٢ – نهلا المومني، قانون جرائم أنظمة المعلومات والحق في الحياة الخاصة ، المركز الوطني لحقوق الإنسان .

٣ – جعفر محمود المغربي ، حسين شاكر عساف ، مرجع سابق ، ص ص ، ٤١-٤٢ .

* جمع معلومات و بيانات عديدة تتعلق بالوضع المادي والصحي والعائلي والعادات الاجتماعية للأفراد ، عبر شبكات الاتصال بطرق التجسس و القرصنة الاليكترونية و تخزنها ومعالجتها ونقلها بسهولة كبيرة مما يشكل انتهاكاً لخصوصية الأفراد ورغبتهم بعدم معرفتها من قبل الغير، و استغلالها بطرق غير شرعية.

* انتحال الشخصيات عبر شبكة الإنترنت للقيام بعمليات النصب و الاحتيال ، و عادة ما يكون ضحيته الكثير من مستخدمي الإنترنت و عادة ما تؤدي جريمة انتحال الشخصية إلى الاستيلاء على الأرصدة البنكية أو السحب من البطاقات الائتمانية وسرقة الحسابات المصرفية أو الإساءة إلى سمعة الضحية.

* جمع البيانات الشخصية و إعادة استغلالها بأساليب تمس الحياة الخاصة كصورة جديدة للاعتداء.

المقصود بجمع البيانات : إن استخدام الحواسيب في ميدان جمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد خلف آثارا إيجابية عريضة ، لا يستطيع أحد إنكارها خاصة في مجال تنظيم الدولة لشؤون الأفراد الاقتصادية والاجتماعية والعلمية وغيرها ، وهذا ما أوجد في الحقيقة ما يعرف **"بنوك المعلومات"** قد تكون مقصورة على بيانات ومعلومات تتصل بقطاع معين، كبنوك المعلومات القانونية مثلا ، أو قد تكون شاملة لمختلف الشؤون والقطاعات ، وقد تكون مهيأة للاستخدام على المستوى الوطني العام كمراكز وبنوك المعلومات الوطنية أو المستخدمة على نحو خاص كمراكز وبنوك معلومات البنوك ، وقد تكون كذلك مهيأة للاستخدام الإقليمي أو الدولي كمراكز وبنوك معلومات الشرطة.. وبفعل الكفاءة العالية لوسائل التقنية والإمكانات غير المحدودة في مجال تحليل واسترجاع المعلومات ، اتجهت جميع دول العالم بمختلف هيئاتها ومؤسساتها إلى إنشاء قواعد البيانات لتنظيم عملها [1] ، واتسع على نحو كبير استخدام الحواسيب لجمع وتخزين ومعالجة البيانات الشخصية لأغراض متعددة فيما يعرف ببنوك ومراكز المعلومات الوطنية ، ومع تلمس المجتمعات لإيجابيات استخدام الحواسيب في هذا المضمار ظهر بشكل متسارع أيضا الشعور بمخاطر تقنية المعلومات وتهديدها للخصوصية . هذا الشعور نما وتطور بفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية واتساع دائرة الاعتداء على حق الأفراد في الحياة الخاصة مما حرك الجهود الدولية والإقليمية والوطنية لإيجاد مبادئ وقواعد من شأن مراعاتها حماية الحق في الحياة الخاصة ، وبالضرورة إيجاد التوازن بين حاجات المجتمع لجمع وتخزين ومعالجة البيانات الشخصية[2] ، وكفالة حماية هذه البيانات من مخاطر الاستخدام غير المشروع لتقنيات معالجتها.

٢ : الاستثناءات التي ترد على الحق في حماية الحياة الخاصة:

يتضمن الحق في الحياة الخاصة عناصر كثيرة منها الحق في الاسم الكامل- الصورة – المعلومات الشخصية السرية- البيانات الخاصة ...وهي محمية من كل الاعتداءات بغض النظر إلى نوعها أي حتى إن كانت على دعامة اليكترونية في مواقع

---

[١] – " إن الكثير من المؤسسات الكبرى والشركات الحكومية الخاصة ، تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي أو الصحي أو التعليمي أو العائلي أو العادات الاجتماعية أو العمل ..الخ ، وتستخدم الحاسبات وشبكات الاتصال في خزنها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها ، وهو ما يجعل فرص الوصول إلى هذه البيانات على نحو غير مأذون به أو بطريق التحايل أكثر من ذي قبل ، ويفتح مجالا أوسع لإساءة استخدامها أو توجيهها توجيها منحرفا أو خاطئا أو مراقبة الأفراد وتعرية خصوصياتهم أو الحكم عليهم حكما خفيا من واقع سجلات البيانات الشخصية المخزنة " .

[٢] – **" على سبيل المثال حكومة الولايات المتحدة وفق دراسات جمعت ٤ بليون سجل مختلف حول الأمريكيين ، بمعدل ١٧ بندا لكل رجل وامرأة وطفل ، ومصلحة الضريبة (IRS) في الولايات المتحدة تمتلك سجلات الضرائب لحوالي ١٠٠ مليون أمريكي على حواسيبها ، وتملك الوكالات الفدرالية ثلاث شبكات اتصالات منفصلة تغطي كل الولايات المتحدة الأمريكية لنقل وتبادل البيانات."**

الانترنت و هذا كقاعدة عامة ،غير أنه ليست بحقوق مضمونة في شكلها المطلق ، لأنه ورد عليها استثناء يتعلق ب "**الحق في الإعلام** "، حيث يباح نشر صورة شخص معين أو تقديم معلومات معينة و إن كانت خاصة بتبرير تحقيق مبدأ الحق في الإعلام عن كل الأحداث و الوقائع و الجرائم التي تقع في المجتمع ، و هو مبرر يقع ضد الق في رفض الشخص أو الاعتراض عن نشر صورته أو ذكر اسمه أو تقديم أسراره عبر وسائل الإعلام بكل أشكالها لاسيما المواقع الاليكترونية[1] .

المطلب الثاني : نظام المسؤولية عن الاعتداء الاليكتروني على الحياة الخاصة

أولا- التكييف القانوني لأفعال الاعتداء الالكتروني على الحياة الخاصة:

كما و سبق قوله ، فقد أثر التطور العلمي على جوانب كثيرة من سلوكيات المجتمع بحيث تغيرت أنماط الحياة و تطورت بسبب ظهور الوسائل الاليكترونية للاتصال و الإعلام ، في البعض منها ايجابيا و في البعض الأخر سلبيا ، بحيث أصبحت وسائل كثيرة تتيح الاطلاع على المعلومات الخاصة للغير و التجسس على أسرارهم، و المتاجرة بها في سبيل كسب الربح السريع ، فالكثير من المواقع الاليكترونية تسعى إلى نشر الفضائح والتنافس على الأسبقية في التصريح بالمعلومات الخاصة ببعض الشخصيات لاسيما المشهورة منها والغنية أو الثرية ، أو حتى نشر صورهم الشخصية دون الحصول على موافقتهم وتناقلها في مختلف دول العالم بكل سهولة، منتهكين بذلك "**مبدأ الحق في الخصوصية المضموم دستوريا**"

فمجال مواقع الانترنت واسع وخطير في طبيعة الأفعال التي تنتهك حقوق الملكية الفكرية في شكلها العام و الحق في الخصوصية، خصوصا وأن النصوص القانونية لم تتناولها بصريح العبارة و لم تجرم الاعتداء الاليكتروني بنص خاص بها ، الأمر الذي لاق تعقيدات في مرحلة تحديد طبيعة الفعل القانونية أي التكييف القانوني للاعتداء الاليكتروني على الحياة الخاصة، و تحديد أركان الجريمة لترتيب العقاب المناسب للجاني الذي بدوره يشكل مشكلا أساسيا فيما يخص تحديد هويته.

ولتكييف فعل الاعتداء يمكن أن نعتمد على طبيعة الحق المراد حمايته ، أي الحق في الحياة الخاصة ، هذه الأخيرة التي تشمل كل الحقوق الشخصية أو اللصيقة بالشخصية التي تهدف الى حماية الكيان الأدبي للإنسان الأمر الذي يجعلنا **<u>نكيف هذه الحقوق بالأدبية</u>**، لكن بالنظر إلى جسامة الأضرار في بعض جرائم المعلوماتية التي تمس الحياة الخاصة فهي جريمة يعاقب عليها قانون العقوبات إعمالا لنص المادة ٣٩٤ مكرر ٢ من القانون رقم٠٤-١٥ و التي تنص على أنه: "**يعاقب...كل من يقوم عمدا و عن طريق الغش بما يأتي** :

١-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم .

٢-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم" .

بل وبالنظر إلى بعض العقوبات التي تضمنها القانون السابق لاسيما غلق المواقع الاليكترونية فالاعتداء على الحقوق بموجب نظام معالجة المعلومات أو البيانات دون تحديد طبيعة الحق يجعل كذلك الحق في الخصوصية على المواقع الاليكترونية موضوع حماية **<u>جزائيا</u>**، وهي **<u>جريمة كيفها المشرع الجزائري بالجنحة</u>**. فالحماية المقررة لحرمة الحياة

---

[1] – عايد رجا الخلايلة ، المسؤولية التقصيرية الاليكترونية ، المسؤولية الناتجة عن إساءة استخدام أجهزة الحاسوب و الانترنت ، دراسة مقارنة ، دار الثقافة ، عمان ، ٢٠٠٩ ، ٢١٩.

الخاصة في الدستور إذن هي **حماية دستورية**، وكذلك حماية المراسلات والأحاديث الخاصة باختلاف وسائلها وصورها، وتقرير العقوبات لجرائم المعلوماتية كجرائم المساس بأنظمة المعالجة الآلية للمعطيات و للجرائم المتصلة بتكنولوجيات الإعلام والاتصال، هي حماية فرضتها ظروف التطور التكنولوجي في مجال وسائل المراقبة والتصنت على الأحاديث الخاصة وتسجيلها الكترونياً بشكل يهدد أسرار الحياة الخاصة وحرمتها بخطر حقيقي بغض النظر عن هوية المعتدى سواء أجهزة الدولة[1] ، أو اعتداء الأفراد على حقوق غيرهم.

المطلب الثاني :القوانين التي تحمي الحياة الخاصة عن الاعتداء الالكتروني في الجزائر :

نظم المشرع الجزائري حماية الحق في الحياة الخاصة من كل أشكال الاعتداءات التي يمكن أن تتعرض لها مهما كانت الوسيلة المستعملة في إلحاق الضرر بالشخص، حيث كيف هذه الاعتداءات بالجنحة فيؤسس الحق في الحماية الجزائية بمجرد توافر أركان الجريمة كقاعدة عامة، وقد وردت العقوبات في قوانين مختلفة، وسمح باللجوء إلى القواعد العامة للاستفادة من الحماية المدنية بموجب تأسيس الدعوى على المسؤولية التقصيرية أو المدنية إذا تعذر أو إذا لم تكتمل أر كان الجنحة .

١- حماية الحياة الخاصة بموجب قانون العقوبات :

حاول المشرع الجزائري أن يتماشى مع ما هو معمول به في مجال محاربة الإجرام الاليكتروني باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية، بموجب القانون رقم١٥٠٤ المتضمن تعديل قانون العقوبات، خاصة بسبب التزايد اللا متناهي للاعتداءات على الأنظمة المعلوماتية بتطور آليات الاتصال وظهور مواقع الاليكترونية والانترنت .و قد نصت المادة٣٠٣ مكرر من قانون العقوبات المعدل بالقانون رقم٢٣٠٦ المؤرخ في٢٠٠٦/١٢/٢٠ [2]على ما يلي: "**يعاقب بالحبس من ستة أشهر إلى٣ سنوات كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص ، بأي تقنية كانت و ذلك :**

١-التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية ، بغير إذن صاحبها أو رضاه

٢- التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص ، بغير إذن صاحبها أو رضاه".

ويعاقب على الشروع في ارتكاب نفس الجنحة بالعقوبات ذاتها المقررة للجريمة التامة. وتضيف المادة٣٠٣ مكررا١ ما يلي :"**يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير أو استخدم بأية وسيلة كانت ، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة** .و تصادر كالأشياء التي تستعمل لارتكاب الجريمة بل و تغلق حتى المواقع التي تتم فيها الاعتداءات بل و حتى المحلات التي وقعت فيها الجريمة إذا تمت بعلم صاحبها .

وتضمن القانون رقم١٥٠٤ المؤرخ في٢٠٠٤/١١/١٠ ، المتضمن تعديل قانون العقوبات قسم عنوانه "**المساس بأنظمة المعالجة الآلية للمعطيات** ". حيث نصت المادة ٣٩٤ مكرر منهما يلي: "**يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من ٥٠٠٠٠ إلى ١٠٠٠٠ دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك**"، و تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن

---

[1] ١٢- أنظر المادة ٤ القانون رقم ٠٤/٠٩ المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها التي أشارت الى حالة مساس سلطات الدولة بحق الحياة الخاصة عند القيام بمهمة المراقبة لكشف ارتكاب جرائم المعلوماتية

[2] ١٣- القانون رقم ٠٦-٢٣ المؤرخ في ٢٠٠٦/١٢/٢٠/ يتضمن تعديل قانون العقوبات ، ح رعدد٨٤.

الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "**تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من ٥٠٠٠٠،إلى ١٥٠٠٠٠ دج**".[1] و ذلك مهما كانت قاعة المعلوماتية أو طبيعتها لذلك يمكن أن تندرج ضمن هذه الاعتداءات تلك التي تمس ببعض صور الحياة الخاصة. ونصت المادة ٣٩٤ مكرر٢ على أنه: "**يعاقب...كل من يقوم عمدا و عن طريق الغش بما يأتي** :

١-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم .

٢-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم" .

و تضيف المادة ٣٩٤ مكرر٦ أنه بالإضافة إلى العقوبات الأصلية أي الحبس و الغرامة و بالاحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية : " **يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم ، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها " .**

٢- حماية الحياة الخاصة بموجب قانون الصحافة :

تنص كل القوانين المتعلقة بالصحافة عل أنه تمارس الصحافة مهمتها بحرية في تقديم الأخبار والمعلومات

والتعليقات وتساهم في نشر الفكر والثقافة والعلوم في حدود القانون وفي إطار الحفاظ على الحريات والحقوق والواجبات العامة واحترام حرية الحياة الخاصة للآخرين وحرمتها، بحيث يلتزم كل صحفي بتحري الحقيقة والالتزام بالدقة والحيدة والموضوعية في عرض المادة الصحفية والامتناع عن نشر ما يتعارض مع مبادئ الحرية والمسؤولية الوطنية وحقوق الإنسان وقيم الأمة العربية والإسلامية، خاصة أن آداب مهنة الصحافة وأخلاقياتها ملزمة للصحفي وتشمل احترام الحريات العامة للآخرين وحفظ حقوقهم وعدم المساس بحرمة حياتهم الخاصة، و تنطبق هذه الاحكام على كل أنواع الصحافة حتى الصحافة الاليكترونية التي تقدم خدماتها عبر مواقع الانترنت[2] .

وقد نص المشرع الجزائري على نفس المبادئ في القانون العضوي رقم١٢-٠٥ المؤرخ في١٢/١/٢٠١٢ و يتعلق بالصحافة في المادة٢:"**يمارس نشاط الإعلام بحرية في إطار أحكام هذا القانون العضوي و التشريع و التنظيم المعمول بهما و في ظل احترام:**

-الدستور وقوانين الجمهورية .

-الدين الإسلامي و باقي الأديان .

---

١ – القانون رقم ١٥/٠٤ المؤرخ في ٢٠٠٤/١١/١٠ ، متضمن تعديل قانون العقوبات، ج ر عدد ٧١ .

٢ – تنص المادة ٦٧ من قانون الصحافة على ما يلي " **الصحافة الاليكترونية هي كل خدمة اتصال مكتوب عبر الانترنت ...ينشر بصفة مهنية من قبل شخص طبيعي أو معنوي يخضع للقانون الجزائري، أما نشاط الصحافة المكتوبة عبر الانترنت كل إنتاج موجه إلى الصالح العام و يتكون من أخبار لها صلة بالأحداث ...في حين خدمة السمعي البصري عبر الانترنت هي خدمة اتصال مثل (واب–تلفزيون) و (واب– إذاعة) موجهة للجمهور أو فئة منه يحتوي أخبار ذات صلة بالأحداث .**



-الهوية الوطنية و القيم الثقافية للمجتمع...

-حق المواطن في إعلام كامل و موضوعي

-سرية التحقيق القضائي.

- **كرامة الإنسان و الحريات الفردية و الجماعية"** [1]، وهو نص عام وواضح فيما يتعلق بالحماية المضمونة للحياة الخاصة التي تتعرض للانتهاك عبر مواقع الانترنت من طرف المقالات الصحفية لذلك نصت المادة١١٥ من نفس القانون على أنه:"**يتحمل المدير مسؤول النشرية أو مدير جهاز الصحافة الاليكترونية، وكذا صاحب الكتابة أو الرسم مسؤولية كل كتابة أو رسم يتم نشرهما من طرف نشرية دورية أو صحافة اليكترونية، ويتحمل مدير خدمة الاتصال السمعي البصري أو عبر الانترنت و صاحب الخبر الذي تم بثه المسؤولية عن الخبر السمعي و أو البصري المبث من قبل خدمة الاتصال السمعي البصري أو عبر الانترنت"** .

وهي مسؤولية جزائية لأن قانون الصحافة نص على أن كل الاعتداءات التي سبق الإشارة إليها تكيف بالجنحة، غير أنه حدد مدة٦ أشهر لتقادم الدعوى العمومية والمدنية المتعلقة بالجنح المرتكبة عن طريق الصحافة الاليكترونية تحسب من تاريخ ارتكابها .

٣-حماية الحياة الخاصة في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.

نص القانون رقم٠٩-٠٤ المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة٤ على أنه:" **يمكن القيام بعمليات المراقبة المنصوص عليها في المادة٣ ...للوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة، في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية...وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات، بالنسبة للمساس بالحياة الخاصة للغير"** [2] . والمقصود من النص أن القانون يخول لبعض السلطات المختصة بالقيام بعمليات المراقبة لكل الاتصالات الاليكترونية[3]، بهدف الوقاية من الأفعال الموصوفة بجرائم الإرهاب و التخريب أو الجرائم الماسة بأمن الدولة إذا تلقوا معلومات عن احتمال اعتداء على منظومة معلوماتية لكن في حدود ما يسمح به القانون لاسيما احترام و عدم المساس بالحياة الخاصة للأفراد ، تحت طائلة تعرضهم للعقوبات المقررة في قانون العقوبات الجزائري عن جنحة المساس بالحق في الحياة الخاصة .

٤- حماية الحياة الخاصة بموجب قانون حق المؤلف و الحقوق المجاورة :

يرى معظم الفقه أن "**الموقع الاليكتروني مصنف متعدد الأغراض**"، يتم استخدامه من الشركات التجارية كعلامة تجارية لتمييز منتجاتها المعروضة للتسويق أو للدعاية عن غيرها على شبكة الانترنت، أو كاسم تجاري أو شعار لجذب الجمهور، كما يمكن أن يستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم السينمائية أو لوحاتهم الزيتية

---

[1] – قانون عضوي رقم ١٢/٠٥ ، مؤرخ في ٢٠١٢/٠١/١٢، يتعلق بالصحافة، مرجع سابق .

[2] – قانون رقم ٠٩/٠٤ ، مؤرخ في ٢٠٠٩/٠٨/٠٥ ،يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، ج ر عدد ٤٧ مؤرخة في ٢٠٠٩/٠٨/١٦ .

[3] – عرفت المادة ٢ من القانون السابق الاتصالات الاليكترونية أنها "...**إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة اليكترونية** " ، مثل الهواتف الخلوية و مواقع الانترنت .



أو العاب الفيديو ...و غيره، وفي كل الحالات يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو اسم تجاري أو مصنف بهدف تحدي هويته عبر الشبكة لكي يعرض ما يريد من سلعة أو خدمة عند إبرام العقد مع إحدى الشركات التي تقدم الخدمات على الشبكة، و بمجرد تسجيل اسم الموقع يحضا بالحماية القانونية المقررة لحق الملكية الفكرية الذي يتضمنه، أي يتحدد القانون الواجب التطبيق حسب الطبيعة القانونية للمواقع فعند تسجيل الموقع كمصنف أدبي أو فني **"لا يجوز أن يعتدي على أي جانب من جوانب الحياة الخاصة للأفراد"** كاستعمال اسم كامل لشخص معين معروف دون الحصول على موافقة من صاحبها أو استغلال صورة أي شخص في الموقع دون الموافقة منه.[1] والمصنف من حيث المفهوم لا ينصرف فقط إلى المادة الملموسة في الخطوط و التماثيل أو اللوحات الزيتية وإنما هي الفكرة المدرجة في المحل الملموس و هي جوهر الإبداع الأدبي أو الفني لأنها الأساس الذي يقوم عليه المصنف أما المادة التي نفذت عليها المادة ما هي إلا وسيلة لنقله إلى الجمهور و قياسا لذلك على موضوعنا تصبح مواقع الانترنت الوسيلة المستخدمة لعرض المصنفات على الجمهور ، و بهذه الصورة فان حماية مواقع الانترنت التي تستغل مصنفا أدبيا أو فنيا على شبكة الأنترنت بقانون حق المؤلف و الحقوق المجاورة[2] ينتج عنه حماية الحق الأدبي و المالي للموقع المسجل كمصنف ، و حماية قانونية لأي حق آخر يتم الإعتداء عليه مثل الحياة الخاصة للأفراد كالحق في الاسم و الصورة و المعلومات الخاصة ...و في كل الأحوال لا يمكن الفصل بين حماية المصنف المستغل في الموقع وحماية الموقع في حد ذاته لأنهم يخضعون لقانون حق المؤلف و الحقوق المجاورة في الوقت نفسه ، لأن حماية الموقع تؤدي بالضرورة إلى عدم الاعتداء على محتوياته بما في ذلك المصنف .

٤- حماية الحياة الخاصة بموجب القانون المدني:

ترتيباً على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة١٢٤ من التقنين المدني الجزائري" **كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض**" وقد جاء هذا النص عاماً وشاملاً لأي اعتداء يقع على أي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة. وقد أورد هذا النص مبدأ مهماً هو حق من وقع اعتداء على حياته الخاصة في التعويض عما لحقه من ضرر فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض." **فالفعل الضار هو أساس المسؤولية**"، وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الاعتداءات الاليكترونية التي تمس بالحياة الخاصة على شبكة الانترنت، وهو عنصر متحول و صعب التحديد في الجرائم التي تمس الخصوصية على المواقع الاليكترونية لما تشكله من صعوبات في الإثبات، وفي تحديد هوية المعتدي[3].وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الاليكتروني الشخصي على أساس الخطأ الواجب الإثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة

---

[1] – و يقول الدكتور الجبوري في هذا الصدد ما يلي:" **من يدخل إلى حاسوبه المرتبط بشبكة الأنترنت معلومات أو برامج بصورة كتابية أو فلما تصويريا أو مقطوعة موسيقية يستفيد من الحماية أيا كانت طريقة العرض "، فالمواقع أو بصفة عامة الانترنت ما هي إلا وسيلة للإتصال و للتعامل مع الجمهور. و لا يرد على الحق في الحماية القانونية بموجب قانون حق المؤلف و الحقوق المجاورة إلا قيد واحد يتمثل في الشروط اللازم توافرها للمطالبة بهذه الحماية و التي تتمثل في شروط حماية الموقع أيا كان الغرض من استغلاله من جهة ، و شروط حماية المصنف الأدبي أو الفني المستغل عبر الشبكة من جهة ثانية. ويقصد عموما بحماية مواقع الأنترنت المسجلة باسم المؤلف الذي يعرض مصنفاته الأدبية أو الفنية على شبكة الأنترنت بقانون حق المؤلف و الحقوق المجاورة"**

– الجبوري سليم عبد الله، الحماية القانونية لمعلومات شبكة الأنترنت ،منشورات الحلبي الحقوقية، ط١ ، لبنان ، ٢٠١١، ص٢٤١ .

[2] – أمر رقم ٠٣-٠٥ المؤرخ في ١٩ جويلية ٢٠٠٣، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر عدد ٤٤ مؤرخة في ٢٣ جويلية ٢٠٠٣.

[3] – عايد رجا العلايلة ، المسؤولية التقصيرية الاليكترونية ، مرجع سابق ، ص٧٢ .

الخاصة بل يجب أن يكون ذلك الفعل الاليكتروني قد وصل إلى درجة الخطأ الذي يشكل اعتداء قابل للإثبات وإن وقع على الشبكة

خاتمة

من خلال استقراء النصوص القانونية نجد بان المشرع الجزائري حاول جاهدا وضع نوع من التوازن ما بين الحق في "**حماية الحياة الخاصة**" و الحق في التفتح على تكنولوجيات الإعلام والاتصال على شبكات الانترنت و المواقع الاليكترونية، والحق في حرية الصحافة ، كما أنه وفر للحياة الخاصة حماية قوية وفعالة ومؤكدة ضد كل انتهاك واعتداء ،وهو ما يؤكد أهمية الحفاظ على حرمة الحياة الخاصة وصيانتها ومكانتها العالية بين الحقوق والحريات الفردية الأخرى ، ونجد بان تطبيق و تفعيل النصوص المتقدم ذكرها أمر كافي للحماية من الاعتداءات التي تمس الحق في الحياة الخاصة مقارنة مع ما وصلت إليه مسألة التطور التكنولوجي و الرقمي و الانترنت في الجزائر مقارنة مع الدول الأخرى على الأقل في السنوات القليلة المقبلة .

و من أوجه حماية الحياة الخاصة القواعد الوقائية الفعالة الإشراف والرقابة بواسطة هيئات مستقلة يعهد لها

١-الإشراف والرقابة السابقة واللاحقة للمعلومات والبيانات المخزنة و منح ترخيص للجهة التي تقوم بعملية جمع ومعالجة المعلومات.

٢- توعية الرأي العام على أن الحقوق والحريات مضمونة حتى عبر مواقع الانترنت ، وكل اعتداء عليها يرتب جزاءات ، بل و وكذلك إرشاد ومساعدة المتضررين في الدفاع عن حقوقهم .

٣- وضع قانون كامل وخاص بالمعلوماتية يكون ثمرة تعاون مشترك بين رجال القانون والمتخصصين في تقنيات الحاسب الآلي ، حتى نضمن الحماية القانونية و التقنية للمعلومات و البيانات الشخصية من جهة، و عدم المساس بالحياة الخاصة من جهة أخرى.

بالإضافة إلى إصدار نص خاص لتجريم استخدام الحاسب الآلي و الانترنت في ارتكاب الأفعال الآتية

١. الالتقاط غير المشروع للمعلومات أو البيانات
٢. الدخول غير المشروع علىأنظمة الحاسب الآلي
٣. التجسس والتصنت على البيانات والمعلومات
٤. انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم
٥. تزوير بيانات أو وثائق مبرمجة أيا كان شكلها
٦. إتلاف وتغيير ومحو البيانات والمعلومات
٧. جمع المعلومات والبيانات وإعادة استخدامها
٨. تسريب المعلومات والبيانات.

قائمة المراجع:

الكتب:

١. الجبوري سليم عبد الله، الحماية القانونية لمعلومات شبكة الأنترنت ،منشورات الحلبي الحقوقية، ط١ ، لبنان ، ٢٠١١.

٢. بسيوني عادل، تاريخ القانون المصري، مصر الإسلامية، مكتبة نهضة الشرق، القاهرة، ١٩٨٥.

٣. عايد رجا الخلايلة ، المسؤولية التقصيرية الاليكترونية ، المسؤولية الناتجة عن إساءة استخدام أجهزة الحاسوب و الانترنت ، دراسة مقارنة ، دار الثقافة ، عمان ، ٢٠٠٩.

٤. خالد ممدوح إبراهيم ، إبرام العقد الاليكتروني، دراسة مقارنة ، دار الفكر الجامعي ،الاسكندرية ،٢٠١١

المقالات:

د/ حسين نوارة ، مظاهر اعتداء مواقع الانترنت على الحياة الخاصة، الملتقى الوطني حول تأثير التطور العلمي و التقني على حقوق الإنسان، كلية الحقوق، جامعة بجاية ، ١٩-٢٠ نوفمبر ٢٠١٣.

النصوص القانونية:

١. أمر رقم ٠٣-٠٥ المؤرخ في ١٩ جويلية ٢٠٠٣، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر عدد ٤٤ مؤرخة في ٢٣ جويلية ٢٠٠٣.

٢. القانون رقم ٠٦-٢٣ المؤرخ في ٢٠٠٦/١٢/٢٠/ يتضمن تعديل قانون العقوبات ، ح رعدد٨٤.

٣. القانون رقم ١٥/٠٤ المؤرخ في ٢٠٠٤/١١/١٠ ، متضمن تعديل قانون العقوبات، ج ر عدد ٧١ .

٤. قانون رقم ٠٤/٠٩ ، مؤرخ في ٢٠٠٩/٠٨/٠٥ ،يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، ج ر عدد ٤٧ مؤرخة في ٢٠٠٩/٠٨/١٦ .

٥. قانون عضوي رقم ٠٥/١٢ ، مؤرخ في ٢٠١٢/٠١/١٢، يتعلق بالصحافة.

البيان الختامي للملتقى الوطني

" آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري"

الجزائر العاصمة ٢٩ مارس ٢٠١٧

نظم مركز جيل البحث العلمي يوم ٢٩ مارس ٢٠١٧ بمقر الإتحاد العالمي للمؤسسات العلمية بالجزائر العاصمة ملتقى وطني حول " **آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري**"،وذلك بالتعاون العلمي مع مخبر بحث الحوكمة العمومية والاقتصاد الاجتماعي بجامعة تلمسان.

و قد شارك في الجلسات العلمية المغلقة أساتذة وباحثون من عدة جامعات جزائرية **أثارت أوراقهم النقص والقصور الوارد** في المنظومة القانونية الجزائرية فيما يخص تنظيم التعامل مع البيئة الإلكترونية،و مست إشكاليات هذا المؤتمر ومختلف محاوره المسطرة،على الشكل الآتي:

المحور الأول: الإطار المفاهيمي للجريمة الإلكترونية.

المحور الثاني: أنواع الجرائم الإلكترونية.

المحور الثالث: الحماية والوقاية من الجرائم الإلكترونية.

المحور الرابع: التشريعات الوطنية في مجال مكافحة الجرائم الإلكتروني.

المحور الخامس: الآليات الوطنية لمكافحة الجرائم الإلكترونية.

ولقد تشكلت اللجنة العلمية التحكيمية للملتقى من السادة الأفاضل:

د.سرور طالبي المل، الأمينة العامة للإتحاد العالمي للمؤسسات العلمية ورئيسة مركز جيل البحث العلمي (مشرفة عامة).

د.أمحمدي بوزينة أمنة/جامعة حسيبة بن بوعلي،الشلف،الجزائر(رئيسًا).

د. رضية بوشعور/ كلية العلوم الاقتصادية،جامعة تلمسان، الجزائر (رئيسة اللجنة العلمية)

د. القص صليحة، جامعة محمد لمين دباغين-سطيف٢.

د. بن غذفة شريفة، جامعة محمد لمين دبلغين-سطيف٢ .

د. بارودي نعيمة/كلية العلوم الاقتصادية،التجارية و علوم التسيير،جامعة أبو بكر بلقايد تلمسان.

د. حسين نوارة/كلية الحقوق و العلوم السياسية،جامعة مولود معمري تيزي وزو.



د. فاطمة الزهرة خبازي، جامعة الجيلالي بونعامة، خميس مليانة.

د. فضيلة عاقلي/جامعة باتنة،الجزائر.

د. محمد بوطوبة/المركز الجامعي غليزان (الجزائر) + مخبر G.P.E.S تلمسان .

د. نادية عمراني، جامعة البليدة٢.

د. يحي برويقات عبد الكريم/جامعة تلمسان.

و قد خلُصت لجنةُ التوصيات إلى مجمُوعة من النتائج هي:

- نظرا لطبيعة الجريمة المعلوماتية الخاصة وكيان بيئتها غير المحسوس تظهر صعوبة مهام السلطات شبه القضائية والسلطات القضائية في أداء دورها للكشف عن الجريمة والبحث عن أدلتها.
- تبقى بعض الصعوبات للكشف عن الجرائم الإلكترونية والمتمثلة في قلة الآثار المادية التي تتركها وكثرة الأشخاص الذين يترددون على مسرحها بين فترة ارتكابها وفترة اكتشافها، حتى وإن نجحت الدّول نسبيا في تطبيق الأساليب الإجرائية التقليدية كالمعاينة والتفتيش والضبط وإضفاء بعض الخصوصيات والشروط لتتلائم وطبيعة الجريمة المعلوماتية.
- جرائم الإنترنت ذات بعد دولي ولا تحدها حدود وطنية أو قومية مما يتطلب تعاونا دوليا للحد منها.
- يستهدف مجرم الإنترنت الإضرار بالآخرين، ويستحق العقوبة بدل عبارات الإعجاب التي تبرز كل ما تتم جريمة جديدة.

واستنادًا إلى هذه النتائج، توصلت اللجنة إلى صياغة جملة من التوصيات، نوردها فيما يلي:

١. ضرورة مراجعة التشريعات الوطنية من خلال تشديد الوصف الجنائي والعقوبات المقررة للأنماط الإجرامية للجريمة المعلوماتية، بغية تحقيق الردع والقضاء على الإجرام المعلوماتي.

٢. ضرورة تعديل بعض التشريعات الجزائرية الحالية وخاصة في مجال الملكية الفكرية بما يتلائم مع طبيعة جرائم الإنترنت، والتقنية، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات وشرحها لهم بشكل واضح.

٣. الإسراع في إصدار القوانين التنظيمية،من خلال وضع مدونة قواعد السلوك في مجال المعلوماتية، تتناسب والتطورات التي يعرفها الإجرام المعلوماتي.

٤. ضرورة إبرام اتفاقات عربية ودولية في مجال مكافحة الجرائم المعلوماتية،وذلك لتحديد إطار الاختصاص القضائي الدولي والتعاون في الكشف وإثبات الجريمة المعلوماتية.

٥. ضرورة إيجاد الوسائل المناسبة للتعاون الدولي لمكافحة هذه الجريمة من الناحية الإجرائية بهدف التوفيق بين التشريعات الخاصة بهذه الجرائم كالتعاون الدولي على تبادل المعلومات وتسليم المجرمين وقبول أي دولة للأدلة المجموعة في دول أخرى لضمان الحماية العالمية الفعالة لبرامج المعطيات الآلية والكمبيوتر وشبكة الانترنت ككل.

٦. مساعدة شركات التقنية والإنترنت في اتخاذ إجراءات أمنية مناسبة،سواءً من حيث سلامة المنشآت أو ما يختص بقواعد حماية الأجهزة، والبرامج.

٧. التنسيق لإنشاء مركز معلومات عربي مشترك يهتم برصد وتحليل جرائم الحاسوب، يضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم.

٨. الاستعانة بمختصين وخبراء قادرين على تشخيص الجريمة والعمل على تكوين فرق من الضبطية القضائية و القضاة مع توفير كافة الوسائل المادية والتقنية اللازمة لها لأداء عملها ومهامها على أحسن صورة.

٩. عقد دورات مكثفة للكوادر البشرية العاملين في حقل التحري والتحقيق، والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوب، والجرائم المرتبطة بها، والنظر في تضمين مناهج التحقيق الجنائي في كليات، ومعاهد تدريب الشرطة موضوعات عن جرائم الإنترنت.

١٠. ضرورة خلق ثقافة اجتماعية جديدة تندد بجرائم الإنترنت مع تفعيل أسلوب التوعية والتهذيب لدى مستخدمي شبكة الاتصالات العالمية وحثهم على الاستخدام الأمثل لهذه التقنيات.

١١. ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة.

١٢. تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحة الجريمة المعلوماتية و الحد من أثارها.

١٣. تشجيع الباحثين بالدعم المعنوي، والمادي، لإجراء المزيد من البحوث والدراسات حول الجرائم المستحدثة.

١٤. رفع توصيات هذا الملتقى إلى الجهات المعنية، ونشرها على نطاق واسع من خلال الصحافة والإعلام، ومختلف مواقع التواصل الاجتماعي.

وفي الأخير يدعو مركز جيل البحث العلمي جميع المشاركين في هذا الملتقى وأعضائه ومتتبعيه، مواصلة البحث ونشر المقالات والدراسات المتخصصة. وبناءً على توصيات لجنة الصياغة بالمؤتمر ستُنشر أعمال هذا الملتقى ضمن سلسلة أعمال المؤتمرات الصادرة عنه.




مركز جيل البحث العلمي
www.jilrc.com
JiL Scientific Research Center